Sirtfi Working Group Update
&
Gathering Input From FIM4R

Scott Koranda
scott.koranda@ligo.org
FIM4R
Vienna, February 2019

Sirtfi

- Security Incident Response Trust Framework for Federated Identity
- "...enable the coordination of incident response across federated organisations."
- Sirtfi v1.0 December 2015 https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf
- REFEDS' Sirtfi Working Group https://wiki.refeds.org/display/GROUPS/SIRTFI

SIRTFI
Security Incident Response Trust Framework for Federated Identity

Sirtfi Working Group Coordinates

- Mailing list subscribe

  https://lists.refeds.org/sympa/info/sirtfi

- Mailing list archive

  https://lists.refeds.org/sympa/info/sirtfi

- Google Drive
  https://drive.google.com/drive/folders/13EhgPxzLy4U6FMP_cVDaIbqju40hOhUR

Tom Barton <tbar… Wed, Jan 30, 12:45 PM (10 days ago)

to sirtfi@lists.refeds.org

Hello colleagues,

Our next call is Thu Jan 31 at 0800CST/1500CET.

https://internet2.zoom.us/j/8853848902

Last time we identified several aspects of federated security incident response that need work and resolution. This time we'll focus on defining next steps towards each of those ends. Action items will be assigned, so it's best to be there to defend yourself! :-)

A more detailed agenda is in the scribing doc.

See you then and there!

Phase 1	Develop the SIRTFI Trust Framework specification, which defines basic security incident response capabilities to which member organizations can self-assert compliance. This initial draft is intended to be a simplified framework that lays the groundwork for how such an approach should be defined. Significant effort will be needed to understand how this might be deployed in the existing R&E FIM environment.	~~Draft SIRTFI document for consultation.~~ ~~Consultation to support development of public v1.0.~~ ~~Decide whether IdP notification of compromised account belongs in v1.0 or will be slated for v2.0 in alignment with Phase 3 work.~~ ~~Propose / finalise entity metadata schema for security contacts~~. ~~Propose / finalise entity attribute profile to signify adherence with Sirtfi public v1.0~~	**COMPLETE** SIRTFI Consultation: Framework Sirtfi v1.0 approved by the REFEDS steering committee and published. Metadata extensions confirmed Guide for Federation Participants Sirtfi added to IANA assurance profiles registry. https://www.iana.org/assignments/loa-profiles/loa-profiles.xhtml

Phase 2	Establish the means by which member organisations in all R&E federations can indicate their compliance with the SIRTFI Trust Framework and how they can be contacted to initiate coordinated response to a federated security incident.	• ~~Produce educational and communication materials for REFEDS to promulgate to member R&E federations.~~ • Promulgate educational and communication materials to help R&E federations to promote and support Sirtfi public v1.0 adoption. • Test incident response process and use of security contact metadata in simulated activity. • Implement processes by which to maintain and broadcast security contact information and Sirtfi trust framework adherence, outside standard federation metadata publication mechanisms. • Establish communication channels for security information exchange and incident report sharing. • Define incident response procedures for federations, including communication templates, and support the community in their adoption. • ~~Implement metadata extension for security contact information.~~ • ~~Implement metadata profile to signify Sirtfi public v1.0 adherence.~~	STARTED Will follow phase 1. Some work incorporated into AARC2 work plan. Homepage https://refeds.org/sirtfi Metadata Guide for Federation Participants GN4-2 will support tools for maintaining security contacts and monitoring adherence Moodle training course for Sirtfi under AARC

Phase 3	Establish the means for proactive notification of an account compromise when it can be expected to produce a substantial impact to an at-risk SP organisation.	• Analyse suitability of existing identity event notification solutions to R&E federations • Define and set up means for IdP organizations to issue events related to account compromises. • Develop tools to help IdPs identify accounts that have been used to access SPs that have registered themselves as being at-risk. • Define Sirtfi version 2 to include the requirement to notify affected participating organisations of security incidents	**PENDING** Will follow phase 2. Work incorporated into AARC2 work plan.

Sirtfi Registry (?)

- Not all federations have matured
  - Not always possible for entities to self assert Sirtfi through federation
- LIGO presented specific use case
  - IdPs in India critically important as LIGO-India has broken ground
  - LIGO would like to require Sirtfi for all IdPs
- Sirtfi Registry proposed solution
  - Allow entities to self assert Sirtfi into a SAML metadata feed
  - Not necessarily (and most likely not) the eduGAIN SAML metadata feed!
- Opportunity to build community tool for reputation based trust
  - entities could be "up- and down-voted" based on incident response experiences
  - LIGO wants to leverage CERN's experiences and vice versa

Sirtfi Registry (?)

- Reception by broader community was...curious...
- Sirtfi Working Group tabled Registry work for now
  - Suggested that LIGO just do the work on its own
  - But...

Community Tagging (a.k. Pixie Dust)

- GÉANT GN4-3 activity
- "Research communities have a need to express and potentially share certain trust marks on IdPs and SPs. These trust marks may differ from existing trust marks issued by identity federations, or may be put in to compliment existing ones, in case the federation operator does not support these, like e.g. in the case of SIRTFI."
- "This project tries to implement a technical solution...It does not consider itself with the questions on where and how such a tool would be used in the context of existing trust frameworks."
- Get in touch with Jule Ziegler, Niels Van Dyke, Uros Stevanovic

Sirtfi Registry/Community Tagging (?)

What say you?

Would your research community leverage a "community tagging" service?

Sirtfi Progress on Research SPs

- 136 SPs assert Sirtfi in eduGAIN metadata (2019-02-11)
- 93 of those 136 registered by InCommon
- What impediments are there?

Other Input for Sirtfi WG Requested

Ideas for means of sharing confidential info among incident responders?

Any unusual suspects among those who may need to participate in response to a federated security incident?