An introduction to Sirtfi
Addressing Federated Security Incident Response

Hannah Short
CERN
hannah.short@cern.ch
• Federated Security Incident Response
  • The problem
  • The solution

• A Security Incident Response Trust Framework for Federated Identity
  • A history
  • Trust Framework Requirements

• How to adopt Sirtfi
  • Metadata
  • Find out more
What if...?

... an incident spread throughout the federated R&E community via a single compromised identity?
Federated Security Incident Response

What if...?

• How could we determine the scale of the incident?
  • Do useful logs exist?
  • Could logs be shared?

• Who should take responsibility for resolving the incident?

• How could we alert the identity providers and service providers involved?

• Could we ensure that information is shared confidentially, and reputations protected?

<table>
<thead>
<tr>
<th>eduGAIN numbers</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Federations:</td>
<td>38</td>
</tr>
<tr>
<td>All entities:</td>
<td>3232</td>
</tr>
<tr>
<td>IdPs:</td>
<td>2037</td>
</tr>
<tr>
<td>SPs:</td>
<td>1197</td>
</tr>
<tr>
<td>Standalone AAs:</td>
<td>3</td>
</tr>
</tbody>
</table>

Data valid as of May 2016
Federated Security Incident Response

The problem

- Clearly an inviting vector of attack
- The lack of a centralised support system for security incident response is an identified risk to the success of eduGAIN
- We will need participants to collaborate during incident response – this may be outside their remit
It all seems like common sense...

SP

SP notices suspicious jobs executed by a handful of users from an IdP

IdP

IdP identifies over 1000 compromised identities

IdP identifies all SPs accessed

Notifies SPs

SP

SP

SP

SP

SP
... but in reality

Large SP does not share details of compromise, for fear of damage to reputation

SPs are not bound to abide by confidentiality protocol and disclose sensitive information

Small IdP may not have capability to block users, or trace their usage

No security contact details!
Federated Security Incident Response
The solution

- Attacks inevitable 😞
- But we can make security capability transparent and build relationships between organisations and people 😊

...We need a trust framework!
# A Security Incident Response Trust Framework

## A history and the future

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FIM4R Paper</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Security for Collaborating Infrastructures (SCI)</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>REFEDS Working Group</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>AARC</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Sirtfi v1.0 Published</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>First Round Deployment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RFC</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>AARC2</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Second Round Deployment</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Images of pentagons and arrows representing the timeline.*

[https://aarc-project.eu](https://aarc-project.eu)
• Issue of IdM raised by IT leaders from EIROforum labs (Jan 2011)
  • CERN, EFDA-JET, EMBL, ESA, ESO, ESRF, European XFEL and ILL
• These laboratories, as well as national and regional research organizations, face similar challenges
• Prepared a paper that documents common requirements
  https://cdsweb.cern.ch/record/1442597

“Security procedures and incident response would need to be reviewed. Today, each resource provider is for example responsible for terminating access by known compromised identities. With identity federation, this responsibility will be shifted to the IdP though resource providers will insist on the ability to revoke access.”

“Such an identity federation in the High Energy Physics (HEP) community would rely on:
• A well-defined framework to ensure sufficient trust and security among the different IdPs and relying parties.”

Credit to David Kelsey (STFC) for this content
A Security Incident Response Trust Framework
Security for Collaborating Infrastructures (SCI)

- A collaborative activity of information security officers from large-scale infrastructures
  - EGI, OSG, PRACE, EUDAT, CHAIN, WLCG, XSEDE, ...

- Laid the foundations for a Trust framework
  - Enable interoperation (security teams)
  - Manage cross-infrastructure security risks
  - Develop policy standards
  - Especially where not able to share identical security policies

- Proceedings of the ISGC 2013 conference
  [http://pos.sissa.it/archive/conferences/179/011/ISGC%202013_011.pdf](http://pos.sissa.it/archive/conferences/179/011/ISGC%202013_011.pdf)

Credit to David Kelsey (STFC) for this slide
A Security Incident Response Trust Framework

Sirtfi status

The SCI document formed the basis for the Security Incident Response Trust Framework for Federated Identity.

This framework has been approved by the REFEDS Community and registered as an assurance profile by the Internet Assigned Numbers Authority (IANA)

https://www.iana.org/assignments/loa-profiles/loa-profiles.xhtml
# A Security Incident Response Trust Framework

## Sirtfi summary

<table>
<thead>
<tr>
<th>Operational Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Require that a security incident response capability exists with sufficient authority to mitigate, contain the spread of, and remediate the effects of an incident.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Incident Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Assure confidentiality of information exchanged</td>
</tr>
<tr>
<td>• Identify trusted contacts</td>
</tr>
<tr>
<td>• Guarantee a response during collaboration</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traceability</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Improve the usefulness of logs</td>
</tr>
<tr>
<td>• Ensure logs are kept in accordance with policy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Participant Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Confirm that end users are aware of an appropriate AUP</td>
</tr>
</tbody>
</table>
## A Security Incident Response Trust Framework

### The benefits

<table>
<thead>
<tr>
<th><strong>IdPs</strong></th>
<th><strong>SPs</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Gain <strong>access</strong> to useful services that only allow authentication from Sirtfi compliant IdPs</td>
<td>Gain <strong>users</strong> whose home organisations only allow authentication at Sirtfi compliant SPs</td>
</tr>
</tbody>
</table>

- Guarantee an efficient and effective **response** from partner organisations during incident response
- Raise the bar in operational **security** across eduGAIN
How to adopt Sirtfi
A simple recipe

• Up to date instructions can be found on the Sirtfi Wiki
  https://wiki.refeds.org/display/SIRTFI/Guide+for+Federation+Participants

• All Federation Entities, including but not limited to IdPs and SPs, can adopt Sirtfi by following this simple recipe
  • Complete a self assessment of your entity following the Sirtfi Framework (all requirements included in the appendix of this presentation)
  • Choose a security contact and include this in metadata
  • Assert Sirtfi compliance by adding a Sirtfi Entity Attribute to your metadata

• Liaise closely with your Federation Operator as they may handle all metadata extensions themselves!
How to adopt Sirtfi
Security contact details

• Who to choose?
  https://wiki.refeds.org/display/SIRTFI/Choosing+a+Sirtfi+Contact
  • Individual/group who will perform Sirtfi requirements on behalf of the entity
    (entity = federated identity-provider/service-provider/...)
  • Can leverage CERTs and other existing external teams

• What to include?
  • Mandatory GivenName and EmailAddress
  • Can add additional telephone numbers and email addresses if desired

<ContactPerson contactType="other"
  xmlns:remd="http://refeds.org/metadata"
  remd:contactType="http://refeds.org/metadata/contactType/security">
  <GivenName>Security Response Team</GivenName>
  <EmailAddress>security@institution.edu</EmailAddress>
</ContactPerson>

Credit to David Groep (Nikhef) for this slide
How to adopt Sirtfi

Security contact choice

Is my organisation Sirtfi compliant?

Yes

Is my organisation covered by an external incident response team?

Yes

Do we wish to leverage this team as primary Sirtfi contact?

Yes

Do they agree to support Sirtfi on behalf of my organisation?

Yes

External Security Team

No

No

No

Improve operational security practices

No

Does my organisation have a computer security (or equivalent) team?

Yes

Does this team have sufficient FIM knowledge to support Sirtfi?

Yes

Organisation’s Security Team

No

No

Do Entity Operator representatives have security knowledge?

Yes

Entity Operator Team or Individual

No

No

No
Framework requirements

- Use and respect the Traffic Light Protocol (TLP) during all incident response correspondence
- Promptly acknowledge receipt of a security incident report
- As soon as circumstances allow, investigate incident reports regarding resources, services, or identities for which they are responsible

The Sirtfi contact should be the primary point of contact during incident response and is expected to involve secondary contacts as necessary
How to adopt Sirtfi
Expressing compliance

• Assert compliance via standard OASIS assurance profile specification

```xml
<attr:EntityAttributes>
  <saml:Attribute
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    Name="urn:oasis:names:tc:SAML:attribute:assurance-certification">
    <saml:AttributeValue>https://refeds.org/sirtfi</saml:AttributeValue>
  </saml:Attribute>
</attr:EntityAttributes>
```
How to adopt Sirtfi
Find out more – Home Page

The Security Incident Response Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response across federated organisations. This assurance framework comprises a list of assertions which an organisation can attest in order to be declared Sirtfi compliant.

REFEDS' Sirtfi Working Group has been active since 2014 and combines expertise in operational security and incident response policy from across the REFEDS community. Work to publish and implement the Sirtfi Trust Framework is supported by the AARC Project.

https://refeds.org/sirtfi
How to adopt Sirtfi
Find out more – Technical Wiki

https://wiki.refeds.org/display/SIRTFI/SIRTFI+Home
Conclusions

• The Security Incident Response Trust Framework for Federated Identity (Sirtfi) has been developed to address the gap in security response capability within federated computing.

• By creating a sub-network of security conscious entities, and providing contact information for each member, the group raises its mutual trust and is able to establish contact with each other should the need arise.
Thank you
Any Questions?

hannah.short@cern.ch

https://aarc-project.eu

© GÉANT on behalf of the AARC project.
The work leading to these results has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).
Appendix, Sirtfi Assertions
Operational security

- [OS1] Security patches in operating system and application software are applied in a timely manner.
- [OS2] A process is used to manage vulnerabilities in software operated by the organisation.
- [OS3] Mechanisms are deployed to detect possible intrusions and protect information systems from significant and immediate threats.
- [OS4] A user’s access rights can be suspended, modified or terminated in a timely manner.
- [OS5] Users and Service Owners (as defined by ITIL [ITIL]) within the organisation can be contacted.
- [OS6] A security incident response capability exists within the organisation with sufficient authority to mitigate, contain the spread of, and remediate the effects of a security incident.
Incident response

• [IR1] Provide security incident response contact information as may be requested by an R&E federation to which your organization belongs.

• [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.

Traceability

• [TR1] Relevant system generated information, including accurate timestamps and identifiers of system components and actors, are retained and available for use in security incident response procedures.

• [TR2] Information attested to in [TR1] is retained in conformance with the organisation’s security incident response policy or practices.
Participant responsibilities

- [PR1] The participant has an Acceptable Use Policy (AUP).
- [PR2] There is a process to ensure that all users are aware of and accept the requirement to abide by the AUP, for example during a registration or renewal process.