short url: http://goo.gl/hg0Uii

A Security Incident Response Trust Framework for Federated Identity (Sirtfi)

Editor: David Kelsey, STFC Rutherford Appleton Laboratory, UK.

DRAFT DOCUMENT (not yet approved or adopted)

Additional authors

Version 1.7.1, 22 October 2014 (include edits by Leif Johansson)

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.

~~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.~~

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.

Background (to be deleted before publication)

To get started we will identify a number of IdPs at willing key Universities or Labs for the research community to implement this trust framework in its draft form and signal such adoption in metadata.

- At this time, only address security incident response
- Needs to be light-weight
- IdPs self assert
- Federation Operators act as conduits of information from IdPs
- Use eduPersonAssurance or “SAMLAuthenticatonContextClassRef” in assertions from IdP http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.html
- Agree to use a separate profile of this for IdPs
- Would be useful to have a filtered metadata aggregator
- There is no defined security contact in metadata so we could use abuse@idp.example.com or just use the technical contact or abuse@scope or
    - https://spaces.internet2.edu/display/InCFederation/Contacts+in+Metadata

Need to clearly define the scope, is it IdP or also AA? What about metadata handlers?

- Attestation of this doc should not jeopardize the attester in light of varying legal or compliance obligations they are subject to.
- This is for consideration by organizations operating IdPs and/or SPs.
-

Introduction

Trust Federations, which provide foundation services that enable authentication and authorisation systems to extend across organisational boundaries, are operated within many nations in support of their Research and Education (R&E) sectors and others. This capability allows Service Provider (SP) organisations to extend access rights to their resources to users whose credentials are managed by Identity Provider (IdP) organisations. Thousands of organizations around the world are members of R&E Federations, and their number continues to grow.

While extremely valuable for large scale collaboration that is a characteristic of R&E activities, this approach also exposes a new vector of attack on SP resources. Since one user credential may have access to SPs at multiple organisations, it presents a way to leverage a compromise at one organisation into an attack on others. The global scale of the overall federated access management system also poses a new challenge to ability to respond to security incidents. How can one organisation know how, or even whether, to contact another to coordinate response to a security incident, and why should they trust each other in so doing?

~~In recent years we have seen the implementation of a variety of infrastructures supporting distributed computing environments and sharing of resources. Each such infrastructure consists of distributed computing and data resources, users (who may be organised into separate user communities), and a set of policies and procedures. Examples of such~~

~~infrastructures include computing grids and/or clouds, as well as cooperating computing facilities managed by different organisations.~~

~~Even when such an infrastructure considers itself to be decoupled from other infrastructures, it is in fact subject to the same threats and vulnerabilities as other infrastructures because of the use of common software and technologies. Moreover, there may be users who use more than one such infrastructure and are thus potential attack-vectors from one infrastructure to another. Finally, one infrastructure may want to extend rights to use its resources to users who are enrolled in a different infrastructure. In each of these situations, the infrastructures can benefit from working together and sharing information on security issues.~~

Security in a distributed collaborative environment is governed by the same principles that apply to any other managed IT-system, but is complicated by the diversity of sites (both in terms of hardware and software systems and in terms of local policies and practices that apply), and by the lack of a centralised governance structure that can mandate operations to be performed in specific ways.

The Sirtfi trust framework is a means by which to enable a coordinated response to a security incident in a federated context that does not depend on a centralised authority or governance structure to assign roles and responsibilities for doing so. This 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.

Governing principles for distributed collaborative environments include:

- The management of risk; both in order to mitigate the most likely occurring and dangerous risks, while adopting countermeasures and other controls that are commensurate with the potential impact.
- Limiting the impact of a security incident while keeping services operational, recognizing that in certain cases the appropriate response is identify and addressing a security vulnerability before re-enabling user access
- Identifying and addressing the root cause of incidents.Identifying users, hosts and services, and controlling their access to resources, all of which must be sufficiently robust and commensurate to the value of the resources and the level of risk and must comply with the regulatory environment
- Active monitoring to detect and reduce the impact of security incidents

~~We encourage openness and transparency in the documentation and for Levels 2 and 3 we recommend that wherever possible documented practice should be made available to collaborating DITIs as a way of promoting trust.~~

Glossary

The following terms are defined for use in the SCI document:

Infrastructure	All of the IT hardware, software, networks, data, facilities, processes etc. that are required to develop, test, deliver, monitor,

	control or support *services*.
Distributed IT Infrastructure (DITI)	An *Infrastructure* together with its management, *Resource Providers* and *Service Operators*. It provides, manages and operates (directly or indirectly) all the *services* required by the *Resource Providers* and their collections of *users*.
Resource	The equipment (CPU, disk, tape, network), software, middleware and data required to run a *service*.
Service	A means of delivering access to, information about or controling *resources.*
Resource Provider	The smallest *resource* administration domain in a DITI. It can be either localised or geographically distributed.
Service Operator	An entity responsible for the management, deployment and operation of a *service*.
Participant	Any entity providing, using, managing, operating, supporting or coordinating one or more *service(s).*
User	An individual or an organisation who has been given authority to access and use *resources*.

Normative Assertions

In this section we define a set of assertions that each organisation shall self-attest to so that they may participate in the Sirtfi trust framework. These are divided into six areas: operational security, incident response, traceability, participant responsibilities, legalities, and data protection.

An attestation to the assertions in this document refers specifically and only to the statements in this section that are identified by labels within square brackets “[“, “]”.

How comprehensively or thoroughly each asserted capability should be implemented across an organisation’s information system assets is not specified. The investment in mitigating a risk should be commensurate with the degree of its potential impact and the likelihood of its occurrence, and this determination can only be made within each organization.

Operational Security [OS]

Managing access to information resources, maintaining their availability and integrity, and maintaining confidentiality of sensitive information is the goal of operational security. ~~Each of the collaborating DITIs must therefore have the following in place:~~

- [OS1] A security framework addressing issues such as authentication, authorisation, access control, confidentiality, integrity and availability, together with compliance mechanisms ensuring its implementation

- [OS2] Security patches in operating system and application software are applied in a timely manner.~~, and patch application is verified, recorded and communicated to the appropriate contacts~~
- [OS3] A process is used to manage vulnerabilities~~ (including reporting and disclosure)~~ in software operated by the organisation.
- [OS4] Mechanisms are deployed to detect possible intrusions and protect information systems from significant and immediate threats
- [OS5] A user's access rights can be suspended, modified or terminated in a timely manner.
- [OS6] Users and Service Owners (as defined by ITIL) within the organisation can be contacted. ~~The capability to identify and contact clients, e.g. authenticated users or portals, and Service Operators~~
- [OS7] A security incident response capability exists within the organisation with sufficient authority ~~The capability to enforce the implementation of the security policies, including an escalation procedure, and the powers to require actions as deemed necessary~~ to mitigate, contain the spread of, and remediate the effects of a security incident.

Incident Response [IR]

Assertion [OS7] above posits that a security incident response capability exists within the organisation. This section's assertions describe its interactions with other organisations participating in the Sirtfi trust framework.

~~A security incident is the act of violating an explicit or implied information security policy. (which must be defined elsewhere)~~

~~The management of risk is fundamental to the operation of any IT Infrastructure. Identifying the root cause of incidents is essential to prevent them from re-occurring. In addition, it is a goal to contain the impact of an incident while keeping services operational. For response to incidents to be acceptable this needs to be commensurate with the scale of the problem.~~

~~It is imperative that every participant has an organised approach to addressing and managing events that threaten the security of resources, data and overall project integrity.~~

We need general intro for IdPs

~~Each Participant must:~~

- [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 and use the Traffic Light Protocol information disclosure policy.

Traceability (or Logging) [TR]

To be able to answer the basic questions "who, what, where, and when ~~and how~~" concerning a security incident requires retaining relevant system generated information, including accurate timestamps and identifiers of system components and actors, for a period of time.

~~Each participant must have the following:~~

- [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. ~~Mechanisms deployed to provide the traceability of the service usage, by the production, retention, and protection of appropriate logging data, to identify the source of all actions as defined above~~
- [TR2] Information attested to in [TR1] is retained in conformance with the organisation's security incident response policy or practices. ~~The documented scope and specification of the logging data retention period.~~
- ~~[TR3] The capability to identify and contact users. (does this work for SPs?)~~

Participant Responsibilities [PR]

All participants in a group of collaborating DITIs need to rely on appropriate behavior by various actors in both their own and other DITIs. We separate these responsibilities into behavior expected of:

- Individual users
- Collections of users
- Resource Providers and Service Operators

Each DITI must ensure that the various participants are aware that they have these responsibilities.

1 Individual Users

Each DITI must have:

- [PRU1] An Acceptable Use Policy (AUP). The AUP must at least address the following areas: defined acceptable use, non-acceptable use, user registration, protection and use of credentials, data protection and privacy, Intellectual Property Rights (IPR), disclaimers, liability, and sanctions for non-compliance.
  - *Need some examples*
- [PRU2] 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.
- [PRU3] Mechanisms deployed to communicate to their users any additional restrictions or requirements on acceptable use that arise out of new collaborative partnerships

2 Collections of Users

A Collection of users is a group of individuals organised around a common purpose jointly granted access to the Infrastructure. It may serve as an entity that acts as the interface between the individual users and each Infrastructure. In general the members of the Collection will not need to separately negotiate with Resource Providers or DITIs.

Examples of Collections of users include: User groups, Virtual Organisations, Research Communities, Virtual Research Communities, Projects, Science gateways, and geographically organised communities.

Each DITI must have:

- [PRC1] A process to ensure that all Collections of users using their infrastructure are aware of, and accept the need to abide by, various policy requirements
- [PRC2] Policies and procedures regulating the user lifecycle management by the body granting access to services. At a minimum these must address the accuracy of user contact information both for initial collection and periodic renewal

Collections of users must:

- [PRC3] Be aware that they will be held responsible for actions by an individual member of the collection which in turn may reflect on the ability of other members to utilise the infrastructure
- [PRC4] Ensure a way of identifying the individual user responsible for an action
- [PRC5] Keep appropriate logs of membership management actions[1] sufficient to participate in security incident response
- [PRC6] Define their common aims and purposes and make this available to the Infrastructure and/or Resource Providers to allow them to make decisions on resource allocation

3 Resource Providers and Service Operators

The DITI must have policies and procedures in place to ensure that Service Operators understand and agree to abide by expected security standards as defined by the DITI, including:

- [PRR1] Vulnerability patching
- [PRR2] Incident reporting
- [PRR3] Physical and network security
- [PRR4] Confidentiality, integrity, and availability of services
- [PRR5] Retention and protection of appropriate logs

Legal Issues and Management procedures [LI]

DITIs, Resource Providers, Service Operators and collections of users must have policies and procedures, appropriately communicated to all participants, that address legal issues including but not limited to the following:

[1] Examples include but are not limited to: Registration or renewal in a membership system, dynamic authorisation such as acquisition of VOMS attributes, authentication to a Science Gateway or portal, job submission or file transfer initiated by the Collection on behalf of an individual user

- [LI1] Intellectual Property Rights clarifying the rights and obligations of the participants
- [LI2] Liability responsibilities and disclaimers to make the participants aware of their obligations
- [LI3] Software licensing clarifying the rights and obligations of the participants
- [LI4] Dispute handling and escalation procedures
- [LI5] Data Protection responsibilities (also see the next section)
- [LI6] Any additional regulations such as export controls, ethical use, externally imposed data protection and/or access control requirements

Protection and processing of Personal Data/Personally Identifiable Information [DP]

DITIs, Resource Providers, Service Operators and collections of users must have policies and procedures addressing the protection of individuals with regard to the processing of their personal data (PII) collected as a result of their participation in the infrastructure, including but not limited to:

- [DP1] Accounting Data
- [DP2] User Registration Data
- [DP3] Monitoring Data
- [DP4] Logging Data
- [DP5] Data owned by or produced by Users or Collections of Users