short url: http://goo.gl/2xnf2G

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

Editor: David Kelsey, STFC Rutherford Appleton Laboratory, UK.
This is a DRAFT DOCUMENT (not yet approved or adopted)

Additional authors

Version 1.8, 29 January 2015 (addressing all edits and suggestions by Tom Barton) - as agreed at video conference on 29 Jan 2015

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

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?

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.

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 four areas: operational security, incident response, traceability and participant responsibilities.

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.

- [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) 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 [IR]

Assertion [OS6] 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.

- [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.

Traceability (or Logging) [TR]

To be able to answer the basic questions "who, what, where, and when" 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.

- [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 [PR]

All participants (IdPs and SPs) in the federations need to rely on appropriate behavior.

- [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.

References