31-01-2018

Incident Response Test Model for Organisations

Deliverable MNA3.3

Contractual Date:	01-02-2018
Actual Date:	31-01-2018
Grant Agreement No.:	730941
Work Package:	NA3
Task Item:	TNA3.1
Lead Partner:	CERN
Document Code:	

Authors: H. Short (CERN), I. Neilson (STFC), D. Groep (Nikhef)

Contributions from: R. Vinot (CIRCL)

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Abstract

Following work in the AARC Project to define an Incident Response Procedure for Federations, this report focuses on validating the proposal by developing tests that involve IdP, SP, Federation and Interfederation operators in simulated security incident response. In addition, the authors present an overview of technologies and tools that may prove useful for automated incident notification.

Table of Contents

Table of Contents

Introduction

As stated in the FIM4R Paper Published in 2012 [FIM4RV1], “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.” This split of responsibility brings with it a number of challenges for communication between distributed organisations; multiple participants may be required to fully understand the impact of a security incident and to take the necessary measures for its resolution. Defining channels of communication between the parties and ensuring that incident notifications are addressed with sufficient priority is a strong requirement for many Research Communities wishing to increase their reliance upon federated identity [FIM4RV1].

The Incident Response Procedure for Federations deliverable, published by the AARC Project [AARC-IR], proposes a chained model for incident notification that leverages the established relationships between federation participants and their registrars (or federation operators), with eduGAIN providing the relationships between independent federations. The procedure hinges on participating organisations’ compliance with Sirtfi, the Security Incident Response Trust Framework for Federated Identity [SIRTFI].

Due to recent changes in Data Protection Legislation for the EU (GDPR), the federated Research and Education community is seeking to leverage Sirtfi to support data breach notification between organisations [I2-SIRTFI]. It is expected that this will boost adoption of Sirtfi and increase the coverage of security contacts across the community. Data breach notification workflows are an important use case for Federated Incident Response, requiring active engagement from Service Providers in particular.

This report proposes simulated scenarios to test the validity of the model proposed during the AARC project. A second objective is to understand whether an automated notifications tool exists that is suitable for our needs. Although this report focuses on incident response notifications for SAML identity federations, the results shown here may be applicable in context of OIDC Federations, or with standalone Identity Providers. By evaluating the initial model with both ‘full-mesh’ as well as ‘hub and spoke’ federations, it similarly covers the model of propagating information through other bridging elements, such as IdP-SP proxy services operated by communities and infrastructures.

Incident Notification Use Cases

The following use cases demonstrate expected security incidents that may occur within identity federations. This list is not definitive - threats and attack vectors will constantly evolve.

Compromised Identity at an Identity Provider

- An Identity Provider discovers an identity has been compromised for a period of time
- They alert all Service Providers that have been accessed by that identity during that period
- Services may detect abnormal activity by the identity and wish to follow up with the Identity Provider or third parties

Suspicious Activity by a Federated Identity at a Service Provider

- A Service Provider notices suspicious activity from a federated identity
- It alerts the Identity Provider with details of the activity
- The Identity Provider investigates
- Additional workflows for “Compromised Identity at an Identity Provider” should be triggered as required

Data Breach at a Service Provider

- A Service Provider is alerted to a personal data breach affecting federated identities, under GDPR they may be required to inform the people whose personal data may have been breached
- The Service Provider informs the Identity Providers for all affected identities

Considerations for Identity Federations

The following is a draft list of constraints and/or considerations for Incident Response involving federated identities:

1. Affected parties may have no existing relationship between them, federation and inter-federation operators may be needed to bridge communication

2. A user identifier for an individual may vary between services (e.g. eduPersonTargetedID) meaning that involvement of the Identity Provider is unavoidable for a complete impact assessment
3. Data Protection regulations must be respected across multiple legislative domains, care should be taken to preserve the privacy of individuals
4. 24/7 Security coverage is unrealistic for the majority of participating organisations, best effort response during common working hours is a reasonable assumption
5. Deployment of components, or the adoption of tools, across all participating organisations should be avoided if possible as such endeavours are unlikely to succeed if significant effort is required
6. Incident notification procedures may vary between hub-and-spoke and full-mesh federations due to, for example, the location of accounting information

Research and Education Federations provide a unique environment for distributed authentication, along with its own challenges. Although some similarities can be drawn with other global trust federations [IGTF], the level of heterogeneity between participating organisations is increased whilst the degree of central operational support is diminished. To address the former, Sirtfi aims to set a lower limit for the heterogeneity of the security capability of federation participants. For the latter, using complementary approaches, both ongoing projects AARC and GN4, through REFEDS, aim to understand the appropriate level of operational support required in the federation landscape.

Automated Notification

It is expected that email communication will be used, at least initially, for incident notification and subsequent communication. However, as reliance upon identity federations grows and the number of authentications increases, an automated notification mechanism may be the most appropriate way to provide coverage of all security events. In this section we provide an overview of relevant standards and tools that may prove useful. Offerings in this area are currently limited.

Security Event Tokens (SET)

The Security Event Tokens (SET) specification draft, as defined by the IETF, proposes a mechanism for communicating facts from the perspective of an issuer about the state of a security subject [SET-DRAFT]. In the context of identity federations a typical use could be a Service Provider issuing a fact about a visiting identity (e.g. a data breach), or an Identity Provider issuing a fact about a managed identity (e.g. a suspected compromise). SETs build on the JSON Web Token format, by adding an “events” claim to contain flexible name and value data pairs relating to the event. There is ongoing work in the Security Events IETF Working Group to define a standard for delivery. It is believed that there are no existing tools that leverage SETs.

When considering the applicability of SETs to the Identity Federation landscape, attention must be paid to protect the privacy of individuals. This may require SETs to only be exchanged along the chain of authentication used by the user originally. A result of this may be the need for widescale deployment of endpoints suitable for exchanging such tokens, a situation best avoided for the sake of ease of deployment. The heterogeneity of identifying attributes will play an important role in defining token format and exchange mechanisms. For example, TargettedID is unique to an SP and by its nature requires IdP involvement to analyse whether the same identity has accessed additional SPs. The SET Audience and Subject will need to be defined with the needs and use cases of the community in mind and it is expected that significant consultation will be required prior to adoption.

MISP

MISP, the Malware Intelligence Sharing Platform, is an open-source Threat Intelligence Sharing Platform [MISP]. The purpose of MISP is to share Indicators of Compromise (IOCs) pertaining to ongoing attacks between organisations; typically these IOCs contain network information or file hashes that an organisation could monitor across their systems. There is already some support in MISP for IOCs regarding individuals or identities, such as passport number or a twitter or github ID. MISP Taxonomies can be created by communities of interest. We discussed the potential to use MISP for incident notification in identity federations with CIRCL, the platform developers.

In contrast to MISP's usual use cases, where IOCs of ongoing attacks are shared to be used by an organisations' monitoring, identity events would typically be communicated only after a period in which an identity was affected. It is likely that the identity would quickly be reset following IOC sharing, assuming that Identity Providers are responsive to blocking identities. MISP Tags can be used to flag IOCs that have been cleared up in this way.

How could MISP work in Identity Federations?

- A taxonomy could be defined for federated identity events, including an object to describe identities
- A dedicated set of MISP instances (or a shared instance for those unable to support one) could be established for the community
- To enable useful sharing of events it is likely that an opaque ID, consistent across organisations, would be required
- Policies would need to be established regarding
    - Privacy protection
    - Authoritative sources of information regarding identity compromises, and account reset (this information may come from multiple sources)

Testing Incident Response

To test the validity of the AARC approach to incident response notification, we propose the following scenarios be simulated. It is expected that email will be the primary communication tool. In this report we provide an analysis of a series of flexible tests, in order to shed light on the reality of incident response in a federated environment. The objective is to test the process, rather than the performance of any of the participants.

Test Description

Test Participants

Volunteer participants should be identified, covering both Full-Mesh and Hub-and-Spoke architectures. The participating IdPs and SPs should be compliant with Sirtfi.

Federation operators should also be approached to confirm their willingness to be involved, as well as interfederation operators where applicable.

Test Structure

The test, described below, should be run twice, once purely using Sirtfi contacts from metadata, and a second time involving federation and interfederation operators. An interview should be conducted with the participants following each test.

Test Guidelines

- Participants should be warned in advance (Appendix A)
- All communication should be clearly marked [TEST] in the subject and contain predefined text to clarify that this is a simulated incident
- Sirtfi obligations, including TLP, should be respected
- Test coordinators should be copied in on communication

Test Objectives

- Ease of use of security contacts from Metadata
- Necessity of Federation Operators and/or interfederation Support
- Although the aim is to test the process, we may also gain insight into
    - Usefulness of logs
    - Responsiveness of Participants

Test 1 - Traceability Exercise

Scenario: One Service Provider discovers a malicious user and alerts the Identity Provider of this user. Additional affected services are identified and should be able to see activity by the Identity in their logs.

Script

1. A “malicious” Identity is used to access SPs across multiple federations
2. The Identity does something suspicious at one SP
3. The SP contacts the IdP of the Identity
4. The IdP checks which other SPs the Identity has accessed
5. The IdP contacts the other SPs directly and requests a response
6. SPs respond with confirmation of the activity

Roles

- Identity 1
- SP 1
- IdP1
- SP 2

Aims

1. All SPs are discovered by the IdP
2. The malicious identity is discovered at each SP
3. SPs and the IdP respond to notifications in a reasonable timeframe

Test Communicator Actions

1. Ask Identity 1 to authenticate to SP 1, 2 and perform a specific task at SP1 (e.g. create a malicious indico event)
2. Tell SP1 about the specific action
3. Monitor and close the test
4. Post-test Interview

Test 2 - Data Breach

Scenario: Service Provider to identity all affected identities and report to their Identity Providers.

Script

1. Identities from participating IdPs are used to access an SP
2. A third party informs an SP of a breach of their data
3. The SP identifies all Identities from the participating IdPs that have accessed the service
4. The SP contacts the IdP for each affected Identity
5. The IdP sends a response to the SP

Roles

- Identity 1
- Identity 2
- Identity 3
- SP 1

- IdP 1
- IdP 2
- IdP 3

Aims

1. All Identities are discovered by the SP
2. IdPs respond to notifications in a reasonable timeframe

Test Communicator Actions

1. Ask Identities 1, 2, 3 to authenticate to SP1
2. Tell SP1 that they have had a data breach
3. Monitor and close the test
4. Post-test Interview

Next Steps

It is suggested that a small scale pilot of these simulated scenarios be carried out within the AARC project (see Appendix D) to gain some experience of coordinating such an exercise. To the best of the authors' knowledge, no tabletop security exercises involving identity federations have been completed previously and it is expected that the tests will be adapted with experience.

Organisations expressing compliance with the Sirtfi framework have, so far, done so with no expectation of completing incident response communication tests. To coordinate a wide scale exercise, participants will need to agree to respond to tests in the spirit of the framework. It is suggested that this is included in a future version of Sirtfi, or the supporting documentation, with support from federation and interfederation governance.

Appendix A - Instructions to Testers

Hello,

You have agreed to be a volunteer to test Incident Response in Identity Federations, based on your participation in the Sirtfi framework.

A test will take place during the week of <>. A short list of questions will be sent afterwards to collect your feedback.

Please note the following guidelines for this test:

- All email communication should be clearly marked [TEST] in the subject
- Email communication should include the boilerplate text ***THIS IS A SIMULATED INCIDENT COORDINATED BY AARC***
- All Sirtfi obligations, including TLP, should be respected
- The test coordinators <> should be in Cc on email communication
- Timed notes should be taken to aid with postmortem

The tests will begin by someone from AARC sending an email to alert a participant regarding a security incident. From that point it is up to the volunteers to use Sirtfi contacts, federation operators, and the eduGAIN support platform support@edugain.org, to fully explore the scope of the incident. We will tell you when the test is over.

Please remember that we are not interested in tricking you or analysing how well your organisation completes the test - the aim is to simulate incident response communication and understand where we need to concentrate effort.

Appendix B - Post-test Interview

The following questions should be asked to each participant following a test.

What went well?

What didn't go well?
Were people responsive?
Were you able to get the information you needed?
Did you need to involve your federation operator? Comment?
Did you need to involve the interfederation support service? Comment?
Would any tools have helped this process?

Appendix C - Test Schedule

It is proposed that the following timeline be adopted for performing the tests. It is recommended to run this twice, once expressly including federation and interfederation operators and again without.

Date	**Action**
Week 1	Share Instructions with Participants (Appendix A)
Week 2	Traceability Test
Week 3	Data Breach Test
Week 4	Post Test Questionnaire (Appendix B)

Appendix D - AARC Pilot, Role Assignment

The following participants have been identified to participate in a preliminary test run, coordinated by AARC. It is recognised that this group represents a small set of sympathetic organisations and may not provide a representative picture of incident response at scale.

Participants

Participant	Role	Federation
CERN User	Identity	SWITCHAAI (Full-Mesh)
INFN User	Identity	IDEM (Full-Mesh)
Nikhef User	Identity	SurfConext (Hub-and-Spoke)
LIGO User	Identity	Internet2 (Full-Mesh)
CERN	IdP	SWITCHAAI (Full-Mesh)
Nikhef	IdP	SurfConext (Hub-and-Spoke)
INFN	IdP	IDEM (Full-Mesh)
LIGO	IdP	Internet2 (Full-Mesh)
RCAuth Certificate Service https://rcdemo.nikhef.nl/getproxy/	SP	SurfConext (Hub-and-Spoke)
CERN Marketplace https://social.cern.ch/community/cern-market	SP (Behind CERN's Proxy)	SWITCHAAI (Full-Mesh)
LIGO	????	Internet2 (Full-Mesh)
IDEM	Federation Operator	
SurfConext	Federation Operator	
SWITCHAAI	Federation Operator	
eduGAIN Support	Interfederation Operator	

Roles

Test	Role	Assigned Participant
Test 1 - Traceability Exercise	Identity 1	INFN Identity
	SP 1	CERN Marketplace
	IdP1	INFN
	SP 2	Nikhef RCAuth
Test 2 - Data Breach	Identity 1	INFN Identity
	Identity 2	CERN Identity
	Identity 3	Nikhef Identity
	SP 1	??
	IdP 1	INFN
	IdP 2	CERN
	IdP 3	NIkhef

References

[FIM4RV1] https://fim4r.org/wp-content/uploads/2017/07/CERN-OPEN-2012-006-2.pdf
[AARC-IR] https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf
[SIRTFI] https://refeds.org/sirtfi
[SEC_EVENT] https://datatracker.ietf.org/wg/secevent/about/
[SET-DRAFT] http://self-issued.info/docs/draft-hunt-idevent-token-07.html
[IR-TESTS] http://www.linuxjournal.com/content/example-security-exercises
[CLAW] https://wiki.geant.org/display/gn42na3/CLAW+Crisis+Management+Exercise
[IGTF] https://www.igtf.net
[MISP] http://www.misp-project.org/documentation/
[TAXONOMIES] https://github.com/MISP/misp-taxonomies
[I2-SIRTFI] https://www.internet2.edu/blogs/detail/15151