26-03-2018

Incident Simulation Report

Continuation of Deliverable MNA3.3

Contractual Date:	N/A
Actual Date:	26-03-2018
Grant Agreement No.:	730941
Work Package:	NA3
Task Item:	
Lead Partner:	CERN
Document Code:	MNA3.3.1

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

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

Abstract

This report describes the results of an Incident Response Simulation of an scenario involving a compromised federated identity accessing multiple services. The simulation was run without an agreed procedure to gather real world feedback on the policy and technical requirements for incident response. It is suggested that the simulation be run again, with an agreed incident response procedure and a new set of participants.

Table of Contents

Introduction

During February 2018 an Incident Response Simulation was coordinated by the AARC Project to better understand the community's needs for Incident Response Procedures and Tooling. Acknowledging that further work to support Sirtfi is ongoing at federations and eduGAIN, it is intended that this exerciseprovide real life justification for policy and tooling choices. The following observations and conclusions will form input to a second iteration of the Incident Response Procedure for Federated Identity [1] proposed by AARC.

Test Methodology

Please read the Milestone document, MNA3.3 Incident Response Test Model, for full information on the proposed simulations for federated incident response [2].

Test Objectives

The test aims to understand the following points

- 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 Script

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

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 let us know if you are unavailable.

Please note the following guidelines for email communication during this test:

- Message subjects should include [TEST]
- Message bodies should include the boilerplate text ***THIS IS A SIMULATED INCIDENT COORDINATED BY AARC***
- The test coordinator <> should be in Cc

The following are recommended for all incidents, including this test:

- All Sirtfi obligations, including TLP, should be respected
- Timed notes should be taken to aid with postmortem

The tests will begin by someone from the AARC project sending an email to alert a participant of a security incident. <If providing a procedure, include details here> From that point it is up to the volunteers to use Sirtfi contacts (and if needed, 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.

Thanks for your participation!

Post-test Interview

The following questions were asked to each participant following the test.

What went well?
What didn't go well?
Were people responsive?
Were you able to get the information you needed?
(for IdPs and SPs) Was federation operator involvement needed? Comment?
(for IdPs, SPs and Federations) Was the eduGAIN support service needed? Comment?
Would any tools have helped this process?
Are there any "lessons learnt" that you would like to share?

AARC Pilot Report

During the AARC Project a pilot Incident Response Simulation was run including volunteer participants spanning four identity federations. The objective was to understand how participants would behave during the Traceability Test when not provided with a procedure. This section provides details on the pilot and its results.

Participants

The following participants were identified. 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.

Participant	Role	Federation	Contact
CERN User	Identity	SWITCHAAI (Full-Mesh)	hannah.short@cern.ch
INFN User	Identity	IDEM (Full-Mesh)	Enrico.M.V.Fasanelli@le.infn.it
Nikhef User	Identity	SurfConext (Hub-and-Spoke)	davidg@nikhef.nl
LIGO User	Identity	Incommon (Full-Mesh)	rtrudeau@ligo.caltech.edu
CERN	IdP	SWITCHAAI (Full-Mesh)	(computer.security@cern.ch), hannah.short@cern.ch
Nikhef	IdP	SurfConext (Hub-and-Spoke)	(cert@surfnet.nl), davidg@nikhef.nl
INFN	IdP	IDEM (Full-Mesh)	(cert@garr.it), Enrico.M.V.Fasanelli@le.infn.it
LIGO	IdP	Incommon (Full-Mesh)	(lsc-seccomm@ligo.org), rtrudeau@ligo.caltech.edu

RCauth Certificate Service https://rcauth.eu/	SP	SurfConext (Hub-and-Spoke)	security@nikhef.nl
CERN Marketplace https://social.cern.ch/community/cern-market	SP (Behind CERN's Proxy)	SWITCHAAI (Full-Mesh)	computer.security@cern.ch,
LIGO Wiki https://wiki.ligo.org/	SP	Incommon (Full-Mesh)	(lsc-seccomm@ligo.org)
IDEM	Federation Operator		(idem@garr.it) barbara.monticini@garr.it, simona.venuti@garr.it
SurfConext	Federation Operator		(support@surfconext.nl) thijs.kinkhorst@surfnet.nl
SWITCHAAI	Federation Operator		(aai@switch.ch) thomas.baerecke@switch.ch
Incommon	Federation Operator		(security@incommon.org) nroy@incommon.org
eduGAIN Support	Interfederation Operator		support@edugain.org

Roles

Test	**Role**	**Assigned Participant**
Traceability Simulation, no procedure	Identity 1	INFN Identity
	SP 1	Nikhef RCauth
	IdP1	INFN

	SP2	CERN Marketplace
	SP3	LIGO SP

Timeline

Rows highlighted indicate the active inclusion of a new participant in the incident. The simulation began on Monday the 19th of February 2018, was allowed to run for a week and was closed by an email from the AARC coordinator on Monday the 26th of February 2018. The decision was taken to end the simulation after one week, despite the incident resolution process being far from complete, since the objectives of this particular exercise had been achieved.

Day	Time (CET)	Action
Day 1	09:05	**SP1 alerted to suspicious activity**
	10:12	**SP1 contacts IdP1's Sirtfi contact**
	10:32	**IdP1's Sirtfi Contact includes IdP1's Federation Operator**
	10:52	**IdP1's Federation Operator contacts IdP1**
	11:29	IdP1's Federation Operator informs SP1 that Identity 1's password has been changed
	12:58	SP1 informs Identity 1 that their token issued at SP1 has been revoked
	15:45	IdP1's Federation Operator sends update to IdP1
	16:32	IdP1's Federation Operator sends update to SP1
	16:43	SP1 asks IdP1's Federation Operator whether any other SPs were affected
Day 2	10:40	IdP1's Sirtfi Contact alerts SP2 and SP3's Sirtfi contacts as well as eduGAIN support
	14:31	**SP2 begins internal investigation**
	16:01	SP2 requests PGP signed mail from IdP1's Sirtfi Contact
	16:17	**eduGAIN encourages response from SP2 and SP3 and includes their federation operators**

	16:31	SP2 tells eduGAIN that they were not officially notified and that a sub-optimal Sirtfi contact was chosen and recommends that an incident coordinator be established
	16:51	IdP1's Sirtfi contact sends SP2 a PGP signed mail including additional information
	17:07	SP2 confirms the incident
	17:31	**SP2's Federation Operator offers help to SP2**
	21:29	**SP3's Federation Operator establishes a secure connection with SP3 and suggests that eduGAIN be incident coordinator**
	21:44	SP3's Federation Operator requests to be contacted at a different email in future, in accordance with their procedure
	21:54	SP2 asks their Federation Operator for advice on coordinating body
	21:49	**SP3's Federation Operator confirms that SP3 is actively investigating**
Day 3	08:22	SP2's Federation Operator proposes eduGAIN as incident coordinator to SP2
	09:50	SP2 seconds SP3's Federation operator's suggestion that eduGAIN be coordinator
	16:06	eduGAIN volunteers to coordinate the incident, assigns incident ID and requests information from all parties
	16:38	SP3's Federation Operator requests that an encrypted channel be established to eduGAIN in order to share information
	17:22	SP1 sends information to eduGAIN without the use of an encrypted channel
Day 4	09:28	SP2 sends information to eduGAIN without the use of an encrypted channel
	13:41	eduGAIN requests information from IdP1's Federation Operator
	13:56	Internal discussions at eduGAIN identity that they do not yet have appropriate tooling but could leverage tools at trusted organisations
	14:34	IdP1's Federation Operator sends information to eduGAIN without the use of an encrypted channel

	15:31	eduGAIN contacts SP2 and SP3's Federation Operator to request that they take over coordination due to lack of tooling
	20:41	SP3's Federation Operator volunteers their messaging platform
Day 5	00:00	SP3's Federation Operator and eduGAIN continue to try to establish an encrypted channel, challenges due to incompatible encryption technologies
	08:20	eduGAIN request that relevant individuals be added to SP3's Federation Operator's messaging platform

Observations

A significant number of problems were observed.

Contacts

1. It was unclear to some parties where the details of Sirtfi contacts could be queried.
2. Many Sirtfi entities list more than one contact, there is no guidance as to which one should be used. There is no differentiation between team contacts (e.g. CERTs) and individuals.
3. Security contacts for federations do not necessarily exist and, where they do, are not documented centrally.

Information flow

1. Critical information, such as Indicators of Compromise, did not reach all parties successfully. As the threads of emails became disjointed and lengthy it became increasingly difficult to create a full picture of the incident. This led to some participants having only a partial picture of the intrusion and lacking crucial details, such as the fact that the initial compromise had been resolved.
2. There was no overall summary due to the lack of a coordinator.
3. Due to the number of ticketing systems triggered, emails swiftly became difficult to follow.

Coordination

1. It was apparent that participants were expecting somebody to take charge. There were many emails including text such as “please let me know how to proceed” despite the lack of an appointed leader during the initial stages of the incident.
2. The incident was not fully investigated initially, and could have remained as a bilateral event had the first service affected not asked explicitly whether others could have been impacted. At later stages, it was unclear to several participants whether the incident had been contained or fully investigated.

Procedure

1. Certain entities wished to use encrypted email while others were content to share information in plain text.
2. Due to lack of clarity on what constituted an “official” notification of an incident, SP2 did not immediately respond.
3. Although a coordinator was established after some time, there was no clear list of its responsibilities, e.g. creating a post mortem and report.

Tooling

1. It became apparent that a secure messaging system was required. Those attempting to send encrypted, or even signed, emails experienced significant delays to communication.

Questionnaire Results

The post-test questionnaire was completed by the test participants. This summary attempts to give an impression of the overall picture of the responses. It should be noted that not all participants have the same working knowledge of incident response, their impressions were provided in the context of their background.

Question	**Response summary (9 responses received)**
What went well?	The initial investigation was quick and responsive and Sirtfi contacts largely worked. eduGAIN support was helpful and included federation operators.
What didn’t go well?	As the incident grew, there was a lack of coordination. Some participants felt that eduGAIN was brought in too late. There was a delay in an official alert to affected services, and no common definition of what constituted an alert.

	It was unclear who should be chosen when multiple Sirtfi contacts are provided. The incident trigger was too vague. It proved impossible to share forensic evidence due to lack of pre-established secure channels. The extent of the incident was not investigated and the full incident response process failed (it should be noted that the process was stopped artificially by the coordinator), participants were not aware that the initial compromise had been contained.
Were people responsive?	General agreement that participants were responsive. Some nudging was needed to overcome timezone and contact choice incompatibilities. Although people were responsive, they did not necessarily have the background in incident response to ask or answer pertinent questions.
Were you able to get the information you needed?	Generally yes, although there was some difficulty in extracting it from email threads. It was unclear to some participants whether the full incident was investigated due to lack of a summary and the absence of a secure channel to share information effectively. More incident specific information was expected, e.g. network layer IoCs. eduGAIN found it difficult to collate all the information. Service Providers would have appreciated receiving further information on IoCs from the other affected participants. Other participants felt that information was readily available. It is suggested that these responses varied according to the working knowledge of the participant regarding incident response; the participants with more mature incident response practices more strongly identified a lack of information.
(for IdPs and SPs) Was federation operator involvement needed? Comment?	Yes, to push the organisations to respond in some cases. Organisations stated that they have more affinity with federation than eduGAIN and their participation provided necessary trusted relationships to progress incident response. In some cases the Sirtfi contact *must* be the federation

	according to federation practices and so their involvement is unavoidable. It was felt that the federation operators would have been essential had the incident's impact grown.
(for IdPs, SPs and Federations) Was the eduGAIN support service needed? Comment?	Yes, although it should be more smoothly coordinated. eduGAIN support proved very useful and alerted the federation operators who might not have been included otherwise. eduGAIN provides the natural coordination point, being the link between all entities, and central coordination would have allowed the incident to be resolved.
Would any tools have helped this process?	Multiple tools were identified: ● Defined, pre-arranged, secure communication channels for both encrypted email and a chat. ● A tool to look up the correct Sirtfi contact for a federated entity was identified as a need by some participants. ● Another participant suggested a single ticketing system instead of emails.

Questionnaire responses also included "Lessons Learnt" that are included here as anonymised quotations:

"I think it would be great to have a general procedure to follow (known by all the eduGAIN support guys) for such an incident. A procedure describing responsibilities of every parties, who to contact in case of emergency."

"A widely known standard process for incidents involving federation (e.g. you should contact your national federation), which should be known beforehand by all national federations so that they can follow-up or discard information as deemed relevant."

"I felt very comfortable dealing with our federation, because I have an existing relationship with them (in particular, with the person I was dealing with). I am not sure I would have felt as comfortable dealing directly with eduGAIN or the federation with the IdP of the compromised credential. Would it be possible to make individual federations part of the scenario automatically, rather than as an escalation?"

“I found this very useful as a first exercise. We should learn from this and, I believe we can agree that we might need an eduGAIN CERT who can take up incident coordination (and eventually help with forensics)!”

“Each federation needs federation-level security contacts, and it needs to be well understood how to get in contact with them. This should be centrally published and coordinated via eduGAIN. We need an eduGAIN CSIRT or something like that.”

“This simulation has been very helpful and based on what we learn last week we would probably change our workflow for what concerns all communications towards other involved parties in eduGAIN”

“As a side comment, we found this very enlightening internally as to shortcomings in our own response infrastructure (some trivially addressed and others that we will need to invest some effort to figure out). I would encourage more of these exercises.”

“The ability to do emergency suspension in the SP using Shibboleth is not widely documented.”

“Responsibilities should be clarified, since there are very different positions in the room. Esp. about the question who should own the global forensic analysis”

“If this was a real incident, I would probably have recommended to block eduGAIN altogether as a precautionary measure.”

Simulation Improvements

Another result of the AARC pilot of this simulation was the identification of possible improvements to the coordination of the tests themselves.

1. Attempt to separate roles as far as possible, for example the IdP operator should not also play the role of the compromised user. It is acknowledged that many individuals play multiple roles in federations, e.g. eduGAIN support and a federation operator, but for the sake of tests it may give greater insight if such overlaps could be avoided.
2. The initial notification of the incident should be credible and provide realistic background information. In this simulation, the evidence pointed to an insider attack because the forensic evidence was not realistic enough to point to a genuine compromise.
3. Define when the simulation will be finished, for example whether this be after a set timeframe of after an incident report has been produced.

Summary

This initial simulation provided insight into the behaviour of interfederation participants during an incident without prior knowledge of an incident response procedure. The incident was terminated by the coordinator after one week. All affected services were identified and the compromised account's password was reset.

The main findings indicate the need for:

- An incident coordinator to be identified early in the incident, with a well defined set of responsibilities
- Federation operators to be included in the incident response procedure to facilitate communication with IdPs and SP
- A secure messaging system, set up in advance
- A well known source of security contacts for federation participants, federation operators and eduGAIN
- Clarity over the use of Sirtfi contacts when multiple are provided
- An incident response procedure for all participants to ensure that expectations are clear, behaviour is consistent and that the incident is fully investigated
- Improved security knowledge at federation participants, federations and interfederation, or access to expertise freely available to the community

Next Steps

It is recommended that this simulation be run again, providing participants with a copy of the incident response procedure [1] proposed during the first AARC project. New participants should be chosen to avoid previous participants learning from their experience.

Whilst the AARC Pilot reported here aimed to highlight incident response needs in a federated environment without coordination or procedures, federations and interfederation are already working towards building incident response capability. These operators should be given time and resources to put in place the required tools and procedures, such as well established eduGAIN support coverage for security, before the next simulation is run.

References

[1] DNA3.2 Security Incident Response Procedure
https://aarc-project.eu/wp-content/uploads/2017/02/DNA3.2-Security-Incident-Response-Procedure-v1.0.pdf
[2] MNA3.3 Incident Response Test Model for Organisations
https://aarc-project.eu/wp-content/uploads/2018/02/MNA3.3-IncidentResponseTestModelForOrganisations.pdf