Sirtfi Communications Challenges, AARC2-TNA3.1

Communications Challenges and incident response models AARC2 NA3 Task 1 - Overview

The Incident Response Procedure for Federations deliverable, published by the AARC Project, 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

In AARC2 we will further the work undertaken in AARC and provide a framework for improving operational security support for inter federation.

Incident response models and guidance

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.

- Incident Response Test Model for Organizations *MNA3.3 (https://aarc-project.eu/wp-content/uploads/2018/02/MNA3.3-IncidentResponseTestModelForOrganisations.pdf)*

Project delivery	AARC2 TNA3.1 project month 9

Communications Challenges and exercises

To test the validity of the AARC approach to incident response notification, we proposed 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.

The first challenge was intentionally performed in an 'open' manner, to assess the effectiveness of merely the Sirtfi security contact meta-data. In the second challenge, participants were provided in advance with a (draft of) the expected response procedure and relevant email templates for communications.

Month	What	Link
10	Incident Simulation #1 Report	https://aarc-project.eu/wp-content/uploads/2018/04/20180326-Incident-Simulation-Report.pdf
19	Incident Simulation #2 Report	https://aarc-project.eu/wp-content/uploads/2018/11/Incident-Response-Test-Model-for-Organisations-Simulation-2.pdf
20	Guideline on Incident Response for Federation Participants	Draft at https://docs.google.com/document/d/1ya4dhp0vzXCcgGinFofVsxQ7wRGxCo4k0S0cR1fl4Us/edit?usp=sharing

Report on incident response

The report provides an overview of the current state of security incident response and cybersecurity in Federated Authentication Scenarios, focusing particularly on efforts that have taken place in the two years related to input from the AARC2 project. It addresses the following elements:

- Incident response based on Sirtfi
- Communications challenges and their future coordination
- Procedure suggestions for federated response
- Security practices for attribute authorities in and beyond BPA models
- The impact of trust groups on federated incident respons

The report was provided as deliverable DNA3.2.

- Report on Security Incident Response and Cybersecurity in Federated Authentication Scenarios
- draft at https://docs.google.com/document/d/1dZX8ua2z40UlekcQ6i88q7mZqEU_4h-dJtygpOUWmH4

Project delivery	AARC2 TNA3.1 project month 21