

ISGC 2024 Security Day

eduGAIN security Table Top Exercise (TTX)

S. Gabriel¹ D. Groep¹ T. Dussa² D. Kouřil^{3,4}
D. Kelsey⁵ M. Kremers⁶ D. Vagheti⁷

¹Nikhef

²DFN CERT

³CESNET

⁴Masaryk University

⁵STFC/RAL

⁶Gèant

⁷GARR

March 25 2024

eduGAIN TTX story

- ▶ Intro to the TTX, get into groups, assign roles to groups.
- ▶ Background, Current Situation.
- ▶ Stage-1, Incident begins, report to IdP/SP Proxy
- ▶ Stage-2, Incident verified
- ▶ Stage-3, Incident spreads
- ▶ Stage-4, Investigation starts
- ▶ Stage-5, Incident handling
- ▶ Stage-6, Incident resolved, close out report

Motivation/Goal

The goal of the exercise:

Raising awareness of the complexity of IR in large/federated environment

Motivation for the TTX

Test IR procedures and policies in eduGAIN and promote/explain the role/utility of eduGAIN CSIRT

Questions to answer

Identify the organisational obstacles in IR, are the available policies complete enough?

Role-play

Why a role-play:

- ▶ Handling a simulated real-life incident affecting a complex environment, to get a better understanding of the risks.
- ▶ "Cheap" way to test available policies and procedures, are they sufficient, do they "work"?

Enabled learning objectives

- ▶ IdP/SP logfile analysis (check for/find a reported Id).
- ▶ know SIRTFI v2, and understand to apply it.
- ▶ Know how eduGAIN is organised, role of Federations, eduGAIN and eduGAIN CSIRT.
- ▶ Name the risks of federated Identity Management.

Roles

Roles, in order of appearance.

- ▶ ISP/SP proxy operator (Fed C)
- ▶ *Fed C operator*
- ▶ IdP A.1 operator
- ▶ Fed A operator ([needed](#))
- ▶ *User*
- ▶ SP B.1 (Cloud compute infra)
- ▶ Fed B operator

Some roles have pretty little to do, can/will be covered by the trainers.

Background, Current situation

Background, Current situation

This game mostly consists of incident elements we handled, though not in the combination we show here.

- ▶ We have a couple of IdP, SP and Federation Operators. All participants have carried out a self assessment and announce to be compliant with SIRT1 v2. (Hey its a perfect world, isn't it :-))
- ▶ Read, discuss your role description, get familiar with your IR tasks.
- ▶ if anything goes wrong, rest easy, finding the obstacles is one of the goals of the play.
- ▶ if anything is unclear, ask us.

What would you do?

During the play you will have to make decisions and report them back to the other players, at each section you should think about what would you do.

When you need information, have instructions for another participants, just raise your hand, we will establish the communication.



Stage-1, Incident begins, report to IdP/SP
Proxy

Stage-1, Incident begins, report to IdP/SP Proxy

IdP/SP Proxy gets a mail from a SP (publisher)with:

A user is massively downloading material. From our logs we see only: 8eceXXXX9382@uni.org I need for example more information about the 8eceXXXX9382@uni.org user, but I don't know how to get it.

- ▶ IdP/SP Proxy receives a request to verify legitimacy of a user, checks the logs.

Stage-1, Incident begins, report to IdP/SP Proxy

IdP/SP Proxy gets a mail from a SP (publisher)with:

A user is massively downloading material. From our logs we see only: 8eceXXXX9382@uni.org I need for example more information about the 8eceXXXX9382@uni.org user, but I don't know how to get it.

- ▶ IdP/SP Proxy receives a request to verify legitimacy of a user, checks the logs.
- ▶ rest of the groups, get used to the concept of an IdP/SP proxy

- ▶ the user identifier is 19382@uni.org, the access to the publisher SP is logged in logs-einfra.txt:

```
Apr 18 08:05:10 login3-d10 proxyaai/simplesamlphp[936]:  
185.177.126.151 einfra NOTICE [ac2e8bef12] User ID:  
134273, identifiers: [eduPersonUniqueId: 8ece13c45965afe  
eduPersonPrincipalName: 19382@uni.org], service: https://  
external identity: 19382@uni.org from https://idp2.uni.c
```

- ▶ maybe one of the participants briefly describes how it works (Marcus?)

- ▶ Taken life time issue

Stage-2, Incident verified

Stage-2, Incident verified

- ▶ translated Id (token to Id) gets reported from IdP/SP proxy to IdP

Stage-2, Incident verified

- ▶ translated Id (token to Id) gets reported from IdP/SP proxy to IdP
 - ▶ The e-infra IdP/SP proxy approaches the uni IdP with the `19382@uni.org` identifier, probably forwarding the complains from the publisher. The Uni IdP establishes the recent activities based on the logs in `logs-uni.txt` (two lines with `19382@uni.org`. They would probably try to check/contact the user and confront them with the AUP violation (which would reveal the compromised account).
- ▶ IdP has a report of an Id potentially involved in activities violating AUP.
- ▶ IdP operator has to decide what to do with this information:
 - ▶ IdP operator to contact user?

Stage-2, Incident verified

- ▶ translated Id (token to Id) gets reported from IdP/SP proxy to IdP
 - ▶ The e-infra IdP/SP proxy approaches the uni IdP with the 19382@uni.org identifier, probably forwarding the complains from the publisher. The Uni IdP establishes the recent activities based on the logs in logs-uni.txt (two lines with 19382@uni.org. They would probably try to check/contact the user and confront them with the AUP violation (which would reveal the compromised account).
- ▶ IdP has a report of an Id potentially involved in activities violating AUP.
- ▶ IdP operator has to decide what to do with this information:
 - ▶ IdP operator to contact user?(y)
 - ▶ User (reliably) denies any relation to the activity in question (DaveK)

Stage-2, Incident verified

- ▶ translated Id (token to Id) gets reported from IdP/SP proxy to IdP
 - ▶ The e-infra IdP/SP proxy approaches the uni IdP with the 19382@uni.org identifier, probably forwarding the complains from the publisher. The Uni IdP establishes the recent activities based on the logs in logs-uni.txt (two lines with 19382@uni.org. They would probably try to check/contact the user and confront them with the AUP violation (which would reveal the compromised account).
- ▶ IdP has a report of an Id potentially involved in activities violating AUP.
- ▶ IdP operator has to decide what to do with this information:
 - ▶ IdP operator to contact user?(y)
 - ▶ User (reliably) denies any relation to the activity in question (DaveK)
 - ▶ To who to report these findings?

Stage-2, Incident verified

- ▶ translated Id (token to Id) gets reported from IdP/SP proxy to IdP
 - ▶ The e-infra IdP/SP proxy approaches the uni IdP with the 19382@uni.org identifier, probably forwarding the complains from the publisher. The Uni IdP establishes the recent activities based on the logs in logs-uni.txt (two lines with 19382@uni.org. They would probably try to check/contact the user and confront them with the AUP violation (which would reveal the compromised account).
- ▶ IdP has a report of an Id potentially involved in activities violating AUP.
- ▶ IdP operator has to decide what to do with this information:
 - ▶ IdP operator to contact user?(y)
 - ▶ User (reliably) denies any relation to the activity in question (DaveK)
 - ▶ To who to report these findings?
- ▶ report to Fed Operator

Stage-2, Incident verified

- ▶ translated Id (token to Id) gets reported from IdP/SP proxy to IdP
 - ▶ The e-infra IdP/SP proxy approaches the uni IdP with the 19382@uni.org identifier, probably forwarding the complains from the publisher. The Uni IdP establishes the recent activities based on the logs in logs-uni.txt (two lines with 19382@uni.org. They would probably try to check/contact the user and confront them with the AUP violation (which would reveal the compromised account).
- ▶ IdP has a report of an Id potentially involved in activities violating AUP.
- ▶ IdP operator has to decide what to do with this information:
 - ▶ IdP operator to contact user?(y)
 - ▶ User (reliably) denies any relation to the activity in question (DaveK)
 - ▶ To who to report these findings?
- ▶ report to Fed Operator
- ▶ What would/should the Fed Operator do with this info?

Stage-2, Incident verified

- ▶ translated Id (token to Id) gets reported from IdP/SP proxy to IdP
 - ▶ The e-infra IdP/SP proxy approaches the uni IdP with the 19382@uni.org identifier, probably forwarding the complains from the publisher. The Uni IdP establishes the recent activities based on the logs in logs-uni.txt (two lines with 19382@uni.org. They would probably try to check/contact the user and confront them with the AUP violation (which would reveal the compromised account).
- ▶ IdP has a report of an Id potentially involved in activities violating AUP.
- ▶ IdP operator has to decide what to do with this information:
 - ▶ IdP operator to contact user?(y)
 - ▶ User (reliably) denies any relation to the activity in question (DaveK)
 - ▶ To who to report these findings?
- ▶ report to Fed Operator
- ▶ What would/should the Fed Operator do with this info?
- ▶ report it to eduGAIN CSIRT? Is it already an (potential) inter-federation incident?

Stage-2, Incident verified

- ▶ translated Id (token to Id) gets reported from IdP/SP proxy to IdP
 - ▶ The e-infra IdP/SP proxy approaches the uni IdP with the 19382@uni.org identifier, probably forwarding the complains from the publisher. The Uni IdP establishes the recent activities based on the logs in logs-uni.txt (two lines with 19382@uni.org. They would probably try to check/contact the user and confront them with the AUP violation (which would reveal the compromised account).
- ▶ IdP has a report of an Id potentially involved in activities violating AUP.
- ▶ IdP operator has to decide what to do with this information:
 - ▶ IdP operator to contact user?(y)
 - ▶ User (reliably) denies any relation to the activity in question (DaveK)
 - ▶ To who to report these findings?
- ▶ report to Fed Operator
- ▶ What would/should the Fed Operator do with this info?
- ▶ report it to eduGAIN CSIRT? Is it already an (potential) inter-federation incident?

Stage-3, Incident spreads

Stage-3, Incident spreads

Compromised Identity is shared with the federation operators

- ▶ What does the IdP hosting the compromised identity do?

Stage-3, Incident spreads

Compromised Identity is shared with the federation operators

- ▶ What does the IdP hosting the compromised identity do?
- ▶ Suspend Identity.

Stage-3, Incident spreads

Compromised Identity is shared with the federation operators

- ▶ What does the IdP hosting the compromised identity do?
- ▶ Suspend Identity.
- ▶ Fed Ops share IoC (compromised Identity) with end entities/Federation Participants (IdPs, SPs)

Stage-3, Incident spreads

Compromised Identity is shared with the federation operators

- ▶ What does the IdP hosting the compromised identity do?
- ▶ Suspend Identity.
- ▶ Fed Ops share IoC (compromised Identity) with end entities/Federation Participants (IdPs, SPs)
- ▶ SPs need to check their logs for IoCs


Stage-3, Incident spreads

Compromised Identity is shared with the federation operators

- ▶ What does the IdP hosting the compromised identity do?
- ▶ Suspend Identity.
- ▶ Fed Ops share IoC (compromised Identity) with end entities/Federation Participants (IdPs, SPs)
- ▶ SPs need to check their logs for IoCs
- ▶ Cloud Compute SP finds IoC

Stage-3, Incident spreads

Compromised Identity is shared with the federation operators

- ▶ What does the IdP hosting the compromised identity do?
- ▶ Suspend Identity.
- ▶ Fed Ops share IoC (compromised Identity) with end entities/Federation Participants (IdPs, SPs)
- ▶ SPs need to check their logs for IoCs
- ▶ Cloud Compute SP finds IoC
 - ▶ The e-infra proxy can identify access to the community proxy (see Apr 18 08:06:31 ... in logs-einfra.txt), which indicates the user might applied for an account with the Community. The logs of community proxy shows access to the Community cloud (see line 2023-04-19T16:30:30.751015+02:00 ... in logs-community.txt.
 - ▶ Just realized we're missing the identifier sent from the Community Proxy to the Cloud (there's only 134273, which is rather external identity). But it's also a real-world example of non-complete logs ;-)
- ▶ Cloud Compute SP checks network connections to VM, 

Stage-4, Investigation starts

Stage-4, eduGAIN CSIRT starts own investigation

(Spoiler, we never did this). Rumours has it that Identities/Accounts are traded on the darkweb <http://abacusmu340oa6hoyg7xic5j2gztky3rplpsbvmqxxk6ywnyqb433poyd.onion>.

Some of us tried to log in, but failed to pass the captcha challenge :- (so no fancy screen shots.

Findings:

- ▶ many Ids from IdP in question are on the marked, selling cheap.
- ▶ checking the software of the IdP in question show its heavily outdated.
- ▶ assumption IdP is compromised

Stage-4, Compromised IdP you say ...

If you need some advise on how this problem **can** be addressed **and** get some international attention, , ask Univ. Giessen:



Bei der Ausgabe der neuen Passwörter kommt es zum Teil zu langen Schlangen. FOTO: LKL © Lena Karber

<https://www.bbc.com/news/technology-50838673>

Stage-4, Situation

Situation:

- ▶ Compromised identity, how it got lost unclear.
- ▶ Moreover, indications that the IdP is controlled by someone else.
- ▶ Identity used at IdP/SP proxy to create an identity (token) which is used at SP-1 (publisher) and SP-2 (Cloud Compute)
- ▶ Compromised identity is suspended at IdP

Stage-4, Situation

Situation:

- ▶ Compromised identity, how it got lost unclear.
- ▶ Moreover, indications that the IdP is controlled by someone else.
- ▶ Identity used at IdP/SP proxy to create an identity (token) which is used at SP-1 (publisher) and SP-2 (Cloud Compute)
- ▶ Compromised identity is suspended at IdP
- ▶ What is the effect of suspending the compromised identity?

Stage-4, Situation

Situation:

- ▶ Compromised identity, how it got lost unclear.
- ▶ Moreover, indications that the IdP is controlled by someone else.
- ▶ Identity used at IdP/SP proxy to create an identity (token) which is used at SP-1 (publisher) and SP-2 (Cloud Compute)
- ▶ Compromised identity is suspended at IdP
- ▶ **What is the effect of suspending the compromised identity?**
- ▶ Started VMs will continue to run until the SP-2 manually suspends VMs

Stage-4, Situation

Situation:

- ▶ Compromised identity, how it got lost unclear.
- ▶ Moreover, indications that the IdP is controlled by someone else.
- ▶ Identity used at IdP/SP proxy to create an identity (token) which is used at SP-1 (publisher) and SP-2 (Cloud Compute)
- ▶ Compromised identity is suspended at IdP
- ▶ What is the effect of suspending the compromised identity?
- ▶ Started VMs will continue to run until the SP-2 manually suspends VMs
- ▶ Created token will remain valid, no means to "revoke" it

Stage-5, Incident handling

Stage-5, Incident Handling

given the situation described in the previous section, groups try to find answers to the following question (10 min):

- ▶ What can/would the Federation Operator of the potentially compromised IdP do?
- ▶ if the Fed Operator suggests the IdP shuts down, IdP Operator explains his/her situation (see [../../supporting_material/compromised_idp_situation.txt](#))
- ▶ What would the IdP operator do (besides reading job adverts)?
- ▶ What can/would eduGAIN CSIRT do?
- ▶ What can/would SP operators do, given they are aware of the situation at the IdP?

Stage-6, Incident resolved, close out report

Stage-6, Incident resolved, close out report (lessons learned

All groups collectively provide input to the close out report:

- ▶ What happened?
- ▶ How was it addressed?
- ▶ Did the procedures work?
- ▶ What to change in the procedures/policies?

Stage-4, Compromised IdP you say ...



<https://www.bbc.com/news/technology-50838673>

