Federated Security Incident Response Policy

C·I·C COMMITTEE ON INSTITUTIONAL COOPERATION
www.cic.net

1819 South Neil Street, Suite D
Champaign, IL 61820-7271
217.333.8475
www.cic.net

February 2011

Contents

Project Participants

Jim Basney ♦ NCSA - University of Illinois at Urbana-Champaign
Mike Grady ♦ University of Illinois at Urbana-Champaign
Matt Kolb ♦ Michigan State University
Rob Stanfield ♦ Purdue University
Von Welch ♦ Indiana University
Keith Wessel ♦ University of Illinois at Urbana-Champaign

1 Incident Response Overview

1.1 Introduction

This document provides a "non-normative" overview of the proposed security incident response (SIR) policy for federated identity environments as put forward by the CIC Identity Management working group TeraGrid pilot (http://docs.google.com/View?id=dcpgz62c_12zb9z48ck).

The policy is not intended to replace existing local IR policy. Rather, it is intended to augment local institutional incident response policies and practices, specifically for inter-institutional incidents that require coordination between two or more institutions.

The policy specifically targets incidents of a security nature and does not attempt to address the complete range of possible incidents in the broad sense of the term (such as defined by ITIL).

The policy is meant to be applicable to the wide array of institutions that comprise an identity federation such as InCommon, including large, medium and small institutions of higher education as well as digital libraries, government agencies, cyberinfrastucture projects and commercial entities.

1.2 Security Incident Response in TeraGrid Today without Federated Identity

To set context, first we present the following workflow, which describes, at a moderate level of detail, an example security incident response (SIR) scenario in the TeraGrid today. Federated identity is not in use in this scenario and the user's home institution is not involved in the user's authentication or directly in the SIR process.

In this scenario a TeraGrid user who normally authenticates to the TeraGrid with a credential such as a password or an SSH private key has had that credential compromised and used illicitly by a third party. It is not meant to describe all possible events, just a typical flow of events, and some details are omitted for simplicity.

1. A TeraGrid user's credentials are discovered to be compromised by one of the sites providing TeraGrid services.
    - This discovery can happen a number of ways: the illicit login can happen from a suspicious IP address, the illicit actor can undertake suspicious behavior (e.g. downloading a known rootkit), etc.
    - The user may be contacted to verify the compromise, or it may be obvious from the behavior.

2. The computer security incident response team (CSIRT) at the site discovering the compromise will deactivate the user's local account (prohibiting further access to the site) and notify CSIRTs at other sites and services comprising the TeraGrid, who will similarly deactivate the account at their sites.

    - CSIRTs will typically look for other activity from the IP addresses involved to see if other accounts may also be compromised, in which case this process repeats for each compromised account.

3. The CSIRT at the site who discovered the compromise will typically take the lead on contacting the user, who will be informed of their compromised credentials and asked to create new ones (e.g. change their password, create a new SSH private key).

    - Contact information for the user is collected when they are enrolled in TeraGrid and stored in the TeraGrid Central Database.

    - The user will be asked a scripted set of questions to help determine the source of the compromise.

    - If there is suspicion that the user's credentials were compromised because their local system is compromised (e.g. their credentials are being repeatedly compromised) they will be asked to engage local site security personnel to investigate that system.

4. Once the user has created new credentials (and restored the integrity of their local system as needed), they are expected to report this fact back to the CSIRT at the discovering site.

5. The CSIRT at the discovering site will re-enable the user's account and inform other sites that they may do the same. The incident is now considered closed.

1.3 Security Incident Response in TeraGrid with Federated Identity

Now we describe how we envision security incident response proceeding under the proposed Federated Identity Security Incident Response policy and procedure. In this case TeraGrid is in the role of a service provider (or SP) and the user is authenticating to TeraGrid using credentials issued to them by their home institution (in the role of an identity provider or IdP). Both institutions are represented in metadata distributed by the InCommon federation.

In this scenario the credentials issued to the TeraGrid user by their home institution have been compromised and used illicitly by an third party. Again, it is not meant to describe all possible possible events, just a typical flow of events, and some details are omitted for simplicity. The main difference with this flow from the previous flow is that instead of interacting directly with the user, TeraGrid (the SP) interacts with the user's home institution (the IdP), who take the lead with user interactions and forensic investigation.

1. Discovery of the compromise by a TeraGrid site happens as in the previous scenario:

    - A TeraGrid user's federated identity credentials are discovered to be compromised by one of the sites providing TeraGrid services. (No change.)

    - The CSIRT at the site discovering the compromise will deactivate the user's local account (prohibiting further access to the site) and notify CSIRTs at sites and services comprising the TeraGrid, who will similarly deactivate the account. (No change.)

2. At this point the flow of events changes. Instead of contacting the user, the CSIRT at the site who discovered the compromise will typically take the lead on contacting the CSIRT at the user's home institution, who wil be informed of their compromised credentials and provided the evidence which led to that conclusion.

    - The user's home institution is obtained by either runtime logs or from information provided by the user when they were enrolled in TeraGrid.

    - Secure contact information (PGP keys, etc.) for the CSIRT at the user's institution is obtained by visiting the SIR URL in the site's metadata (distributed by the InCommon federation). (Note that this contact information is likely different from the administrative contact information for the IdP.)

    - If it is suspected that the user's local system is compromised, that information will be provided as well.

    - The user may also be informed so that they know what is going on.

    The CSIRT at the user's institution will restore the integrity of the user's federated identity credentials (e.g. reset the password and distribute it to the user via some secure channel).

    - They may also undertake other investigations as needed (e.g. seeing if the user's local system or department network is compromised).

    Once the CSIRT at the user's institution are satisfied the user's credentials and local system are restored to a state of integrity, they report this fact back to the CSIRT at the discovering TeraGrid site.

    - If they discovered other information in their investigation that may be pertinent (e.g. other IP addresses that appear to be related or another account that was also compromised and used to access the same service), it is suggested that they share that information with the service provider to the extent allowed by their local policy.

    The discovering TeraGrid CSIRT personnel will re-enable the user's account and notify other TeraGrid CSIRTs as to the resolution. The incident is now considered closed.

1.4 Security Incident Response with Federated Identity and Anonymous Entitled Users

Another interesting use case is when federated identity is used to enable anonymous, but entitled, usage and that usage is abused. For example a service provider may grant access based on a user having a particular role (e.g. staff, student or facility) at a identity providing organization and not receive a unique identifier for the user (we also assume the user utilizes multiple IP addresses, making IP address non-identifying). Now a user abuses the service in some way that represents a security incident - e.g. attempting a SQL injection attack.

In this case, the policy dictates that at a minimum the service provider can take whatever steps locally it desires to protect its service; however, since the service provider cannot uniquely identify the user (or users), those protections may be coarse-grained and impact many users at the identity provider. Under the policy it can locate a security incident response contact at the identity provider and report the misbehavior, providing information about the attacks (time, IP address, etc.). The identity provider should investigate the attacks and take appropriate action as their local policies dictate. They should then respond to the service provider, informing them that the investigation has been completed and appropriate action taken; note that this response is not required to contain any detail (e.g. identity of the user, nature of the action), and in fact policies at the identity provider (e.g. FERPA) may explicitly prevent the sharing of detail.

1.5 Sharing of information for Federated Incident Response

To properly respond to a security incident, an identity provider or service provider may share information about the individual or individuals involved to the respective institution in order to facilitate the investigation of the incident. This information may include the login name, name, dates and times of access, and other information that would be supportive in responding to and resolving security incidents.

While the policy leaves the "what information is shared" up to each organization as they choose based on their respective polices and applicable laws, it does assert that organizations receiving such information shall treat it in confidence, respecting privacy of the individuals involved. To the extent allowed by law, they should not share that information, instead directing any others with a need for the information back to the original institution.

1.6 International Security Incident Response

The grid community has built up significant experience and expertise with coordinating security incident response across national boundaries. As grids (such as the LHC Computing Grid) span national boundaries, so do security incidents. The GRID-SEC organization, with a membership consisting of two representatives of each academic grid infrastructure, provides a top-level forum for security incident information sharing

and coordination across grids. The result is a hierarchical approach to security incident response: sites report incidents to the grid security team, which reports to GRID-SEC, which notifies other grid security teams, who notify their sites as appropriate. The international agreement across grids on the JSPG Security Incident Response Policy (http://www.jspg.org/wiki/Security_Incident_Response_Policy) also facilitates international response.

As inter-federation across today's national-scale federations becomes a reality, international security incident response across federations will be required. The currently proposed Federated Identity Security Incident Response policy does not address international response, but we acknowledge it is an important topic for the future.

1.7 Summary

In summary, introducing federated identity into the incident response scenario makes it more critical for a service provider to interact with the user's home organization to:

- reset the user's credentials,
- locally investigate the compromise,
- coordinate interactions with the user, and
- indicate when integrity has been restored for the user's credentials, so that the service provider can resume normal service for the user.

2 Incident Response Policy

2.1 Introduction

This document describes a security incident response policy in a federated identity environment. It specifically targets incidents of a security nature and does not attempt to address the complete range of possible incidents in the broad sense of the term (such as defined by ITIL).

It was produced by the TeraGrid Pilot project in the CIC Identity Management Taskforce as a proposed policy both for the CIC and the broader InCommon community. This section and "Acknowledgements" are preamble that set the stage for the Proposed Policy, which then follows.

2.2 Acknowledgments

The following documents were used to shape these recommendations:

- JSPG Security Incident Response Policy, version 3.2
- REN-ISAC Membership Guide Document version 2.1, September 22, 2009

Whenever possible, we have used terminology from the InCommon Federation glossary. In particular, we use the following terms as defined in that glossary:

- Identity Provider
- Participant
- Service Provider

2.3 Policy

Goal of this Policy

The goal of this policy is to provide a framework for effective security incident response for a federated environment while avoiding conflict with local laws, policies and contractual obligations that participants are bound to outside the scope of this policy. It specifically targets incidents of a security nature and does not attempt to address the complete range of possible incidents in the broad sense of the term. Specifically, the policy aims to:

1. Define what a "security incident" is in the context of federated identity.
2. Define the roles of the parties involved in federated security incident response: user, identity provider and service provider.
3. Define methods to securely determine who one should communicate with at a particular participant regarding a security incident.

4. Provide common expectations for how security incident response occurs.
5. Establish a philosophy of "do for others as you would do for yourself."

Definition of a "security incident"

1. A security incident is the act of violating an explicit or implied security policy (for example, as documented in an acceptable use policy)
2. A Service Provider is expected to define and provide a service. The expected behavior of a service provider is defined by their Participant Operating Practices (http://www.incommonfederation.org/policies.cfm), and possibly other policies and laws. All SPs are expected to comply with any restrictions contained in sections 2.12 and 2.13 of the Participant Operating Practices of any Identity Provider partners from which they accept identity information. Evidence of behavior by a service provider that violates those policies is considered a security incident.
3. Identity Providers are expected to represent user identities (identifiers and/or attributes) to the degree of authority and accuracy specified in their Participant Operating Practices. Evidence of failure of an Identity Provider to do so, e.g. impersonation of a user by another party, is considered a security incident.

Reporting a Security Incident

1. A participant discovering a security incident should strive to notify any affected parties in the federation to the extent allowed by that participant's policies, relevant laws and resource constraints.
2. The federation shall provide points of contact for participants (Identity and Service Providers) to facilitate security incident response. Participants shall maintain a current point of contact for security incident reporting, in addition to the Technical and Administrative contacts as described in the InCommon Participation Agreement (http://www.incommonfederation.org/docs/policies/participationagreement.pdf) section 6.e, which will be disseminated by the federation. Information should be included or referred to in order to allow for secured communications (e.g. a cryptographic key).
3. Participants, when discovering a security incident, should strive to report the incident to other affected participants at the provided point of contact for security incident response. For example:
4. If an Identity Provider discovers a security incident that affects one or more Service Providers, it should strive to contact those Service Providers and share relevant information.
5. If a Service Provider discovers a security incident that affects one or more Identity Providers, it should strive to contact those Identity Providers and share relevant information.
6. If a security incident involves a user, the incident should be reported to that user's Identity Provider at the provided point of contact for security incident response.
7. Participants should encrypt incident communications to prevent unauthorized disclosure.
8. Service Providers have ultimate authority for access control for their services. A Service Provider may choose to locally de-authorize a user or Identity Provider for any reason, including containment of a security incident.

9. Identity Providers have ultimate authority for access control to their services. An Identity Provider may choose to deny release of user identifiers and attributes to a Service Provider for any reason, including containment of a security incident.
10. A user could be the originator of a security incident report if, for example, they find activity attributed to them at a given Service Provider for which they do not believe they are responsible. The user might report this to either the Service Provider or to their Identity Provider, but in either case, the participant receiving the security incident report should apprise the second participant of the report.

Handling a Security Incident Report

A participant receiving a security incident report ultimately decides what, if any, actions should be taken based on their own resources and relationships with the involved parties. As a goal, a participant receiving a security incident report should strive to treat a security incident report as if it had originated internal to their organization and impacted an internal organizational service, including:

1. Promptly (within one business day), acknowledge receipt of the security incident report.
2. As soon as circumstances allow, investigate incident reports regarding resources, services, or identities for which they are responsible. The participant shall follow its own security incident response procedure, treating an incident with a federated service as if the incident had occurred within a local resource or service.
3. Respond to the incident reporter and any other impacted parties when the incident is resolved. The response should provide sufficient information (as allowed by applicable policies and laws) such that any impacted party can determine their own next step(s). For example, if a user's password was compromised, misused to access a Service Provider, and the integrity of that password now restored, that information would allow a Service Provider to re-authorize access by that user.

Sensitivity of Security Incident Information

During the course of an investigation, information about the incident may be shared between participants.

1. Participants shall aim at preserving the privacy of all involved, and ensure that any confidential or sensitive information is not inappropriately shared.
2. Participants shall not share security incident information on behalf of the federation or any other federation member with external parties such as the media without prior agreement. Inquiries regarding security incidents in the federation should be directed to published federation contact points (http://www.incommonfederation.org/contacts.cfm).

Auditing and logging

1. Participants are expected to keep internal logs with accurate date/time stamps that allow for security incident response. For example, an Identity Provider should be able to identify the specific individual associated with an anonymised identity presented to a Service Provider.
2. Participants are expected to retain such logs for whatever period of time organizational policy dictates or allows.

3 Incident Response Implementation Plan

3.1 Introduction

The intent of this document is to provide guidelines regarding operational procedures associated with Security Incident Response in the context of InCommon Federated activities. Simply put, this document is the how-to companion to the Security Incident Response Policy (SIRP).

3.2 Recommendations

In order to provide an appropriate mechanism to enable the requisite communication in the SIRP, we propose the following recommendations to the InCommon TAC:

1. Include Security Incident Response sections in the POP documents. These sections should include the ability to narratively describe or provide links to institutional Security Incident Response procedures. The proposed changes follow:
    - Modification to 1.3, change "Contact Information" to "Identity Management Contact Information."
    - Add section 1.4 "Additional information about the Participant's Security Incident Response practices and/or policies can be found on-line at the following location(s). URL(s)"
    - Add section 1.5 "Security Contact Information: The following person or office can answer questions about the Participant's Security Incident Response policy or practice."
2. A Security Incident Response contact as an "other" type should be supplied in the InCommon Metadata for each institution. This will allow a way to programmatically provide contact information based on service.
3. Contacts in the Metadata should be extended to include an optional URL attribute for additional information (policies, practices, additional contact information, etc). Example:

```
<ContactPerson contactType="other">
 <Extensions>
  <foaf:workInfoHomepage
xmlns:foaf="http://xmlns.com/foaf/0.1/">http://www.example.com/security-
policy.html</foaf:workInfoHomepage>
 </Extensions>
 <GivenName>Security Incident Reporting</GivenName>
 <EmailAddress>security@example.com</EmailAddress>
 <TelephoneNumber>+1 000 000 0000</TelephoneNumber>
</ContactPerson>
```

Alternatively, an additional Organization URL could be recommended for the purpose of providing Security Incident Response information.

We would also like to recommend that the REN-ISAC be considered as need arises for central management of Security Incident Response. With current federated activities and workload, managing Security Incident Response in a bilateral way between affected IdPs and SPs should be functional, but over time, we could see the need for a centralized approach, and we believe that REN-ISAC could be staffed-up to fit the bill.