XSEDE Capability Delivery Plan
SPI-6: Emergency Account Suspension
Last revised 2017-05-03

Background

Use cases describe community needs, requirements, and recommendations for improvements to cyberinfrastructure “CI” resources and services. A Capability Delivery Plan “CDP” is an executive summary of use case support gaps, of plans to fill those gaps with new or enhanced capabilities, and of existing operational components that already support aspects of a use case.

Use Case Summary

While responding to an account compromise, an **XSEDE operational security team member** needs to temporarily prevent a specific XSEDE user account from being used on XSEDE resources and services.

Use case document(s): https://software.xsede.org/use-case/spi-06

CDP Summary

The functionality described in this use case is not currently supported, i.e., account suspension is currently a manual process in XSEDE.

Gap(s) that we currently plan to address:

- Provide a secure directory of SP Security Admin contacts
- Track status of suspended user accounts
- Provide a secure web interface for emergency account suspension

Gap(s) that will not be addressed at this time:

- None

Time and effort summary:

- 25 total person weeks

Functionality Gaps

1. Provide a secure directory of SP Security Admin contacts (suggested priority: high)

Resource Description Repository (RDR) of XSEDE Central Information Services will be

enhanced to track the security admin contact info, including email addresses, for each of the SP resources. XSEDE User Portal should be able to retrieve the security admin contact info for each of the SP resources.

Best available effort and time estimate: 5 total person weeks

2. Track status of suspended user accounts (suggested priority: high)

The XSEDE Central Database (XCDB) will be enhanced to support tracking of user suspensions. Information on local account suspensions following global account suspension will be tracked also.

Best available effort and time estimate: 5 total person weeks

3. Provide a secure web interface for emergency account suspension (suggested priority: high)

Currently, user account suspension is a manual process, with manual tracking of suspensions. Once this is automated, authorized members of XSEDE Security Operations will be able to login to XUP and suspend a user. XUP will disable the user's kerberos account and update XCDB. XUP will further send a signed email each for each of the local accounts at SPs for the suspended user, to the security admin contacts for that resource retrieved from Resource Description Repository (RDR) of XSEDE Central Information Services. The email will specify a hyperlink to the XUP page where the security admin can update the status of the local account to indicate one of

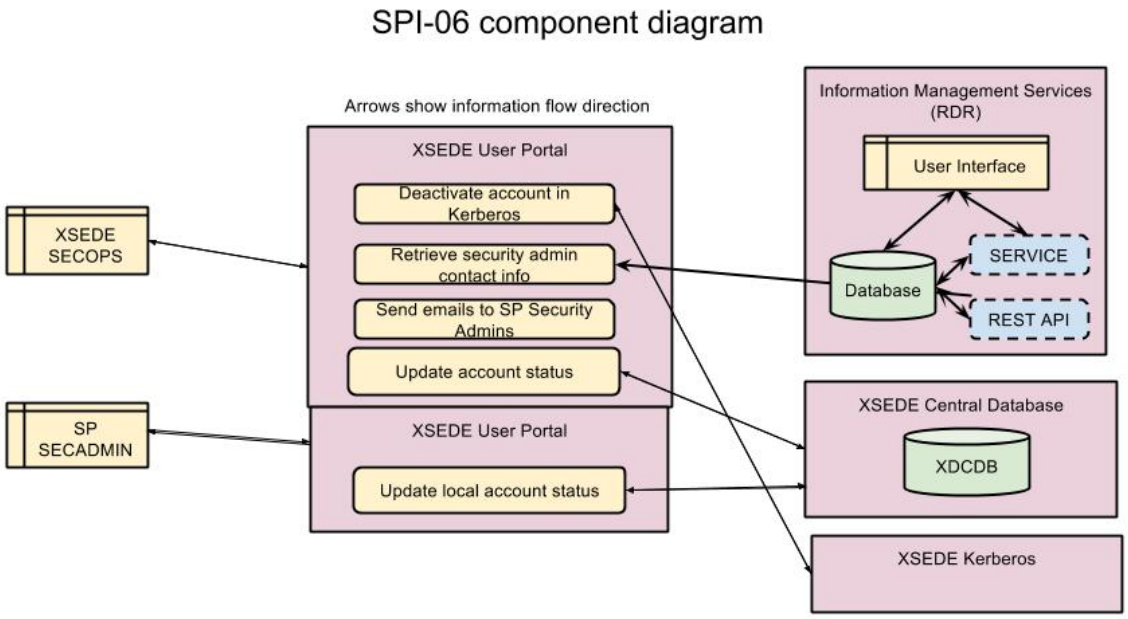
1. local account suspended
2. local account being closely monitored
3. Other free-form text

XSEDE Security Operations will be able to lookup the local account status of a suspended user, as updated by the security admins and would be able to trigger another email to be sent by XUP to SPs that haven't updated the status yet.

XSEDE Security Operations will also be able to "unsuspend" a user in the same way as a user is suspended, triggering emails to be sent to the security admins.

Best available effort and time estimate: 15 total person weeks

System Components That Support This Use Case



The following XSEDE operational components can be modified to support this use case:

(Hyperlink the component <Name> to the XCSR Component Description Repository)

Component	**Supported Functionality**
XCDB	Will be enhanced to track user account suspension with inputs from XUP.
RDR	Will be enhanced to track security admin contact info for SP resources for retrieval by XUP.
XUP	Will be enhanced to allow user account suspension and unsuspension by XSEDE security operations.