PITTSBURGH SUPERCOMPUTING CENTER

BRIDGES
A PITTSBURGH SUPERCOMPUTING CENTER RESOURCE

Flexible Enforcement of Multi-factor Authentication with SSH via Linux-PAM for Federated Identity Users

Derek Simmel dsimmel@psc.edu
Shane Filus filus@psc.edu

PEARC17 - New Orleans, LA
July 13, 2017

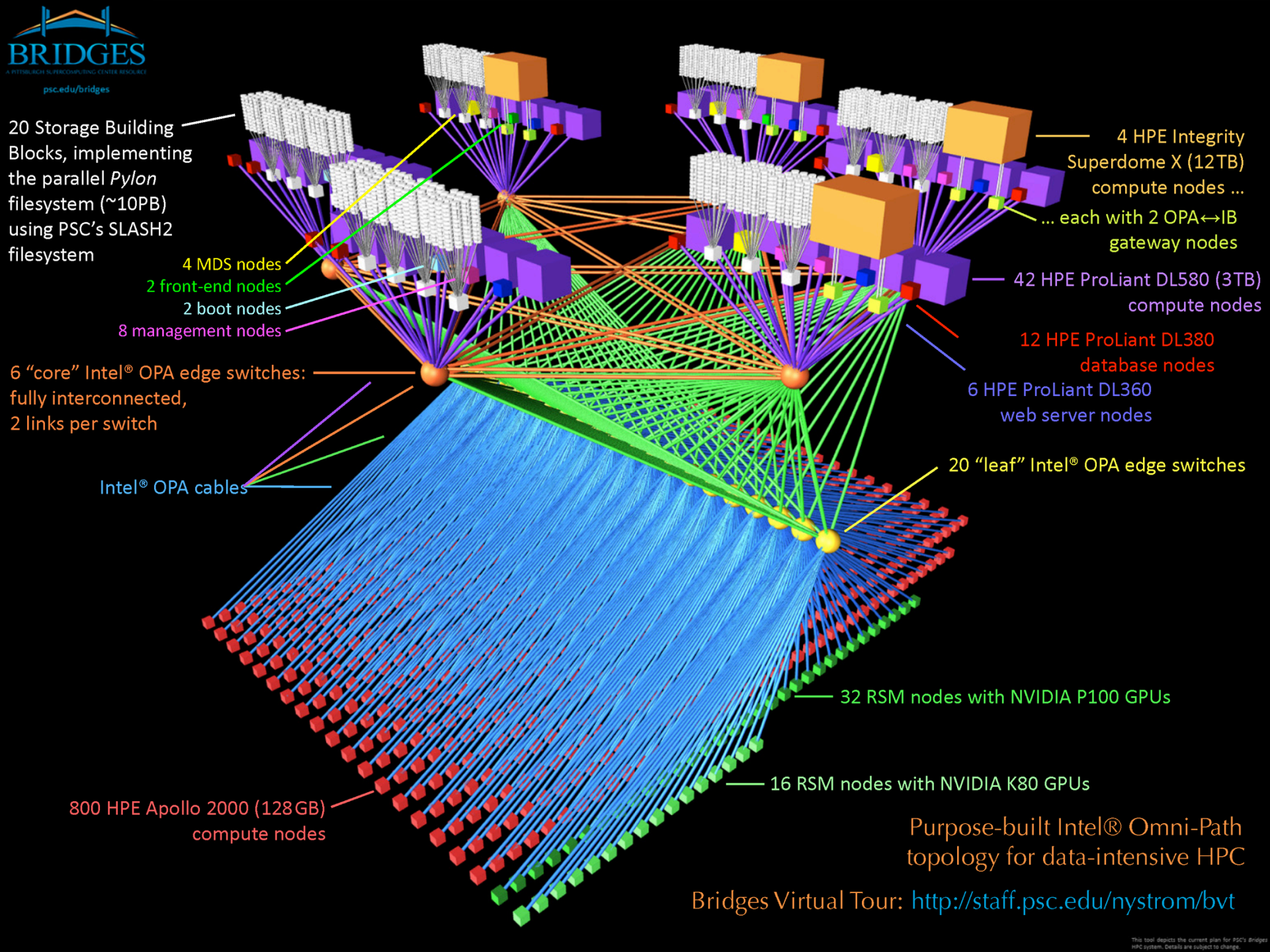
XSEDE
Extreme Science and Engineering Discovery Environment

Flexible Enforcement of Multi-factor Authentication with SSH via Linux-PAM for Federated Identity Users

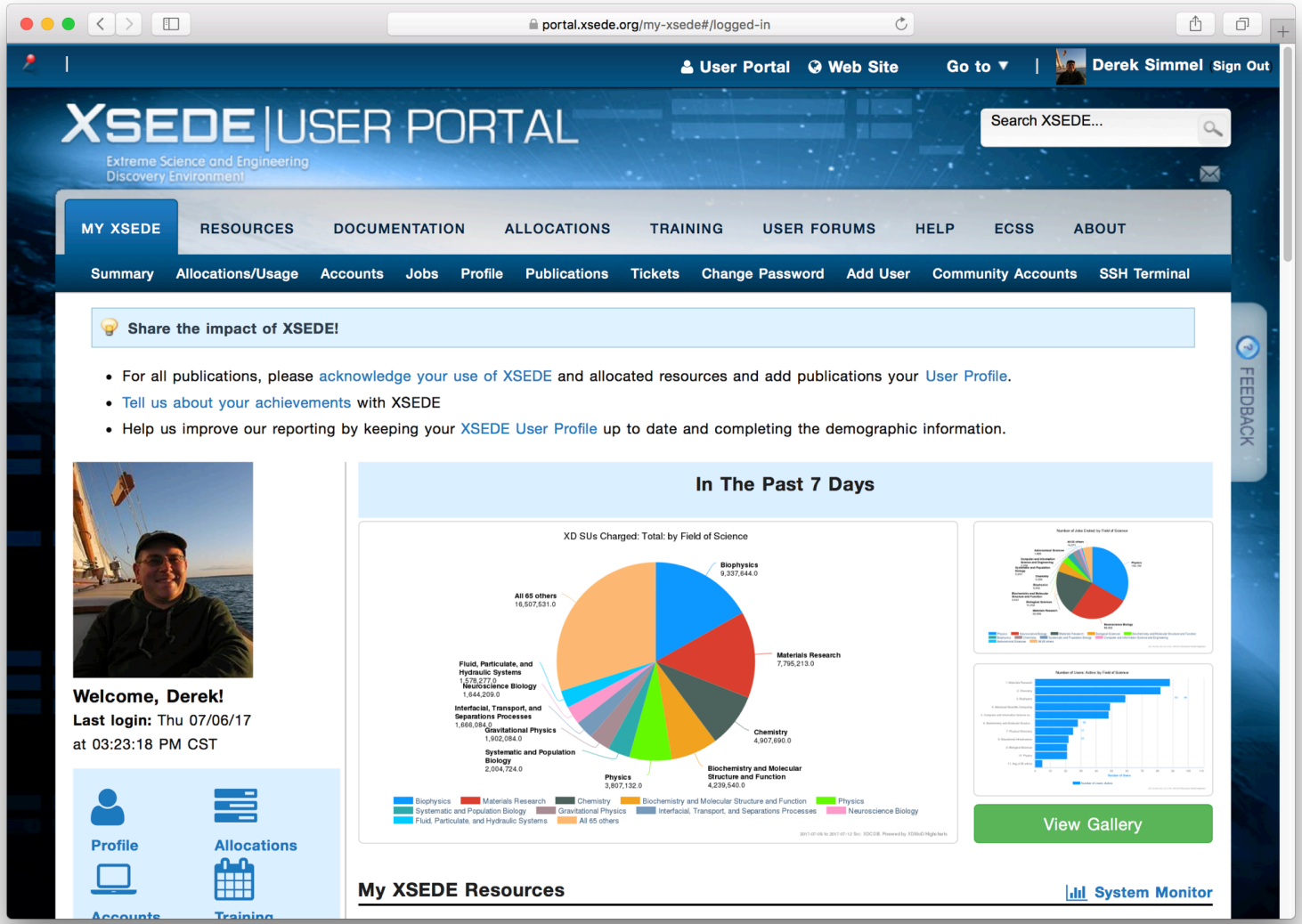
- What use case are we addressing?
  - Some, but not all, XSEDE users **must** use multi-factor authentication to login via SSH to PSC *Bridges*
- SSH, GSI-OpenSSH, XSEDE Single Sign-On, and Duo MFA
- Requirements for Flexible Multi-factor Authentication
- XSEDE Multi-Factor Authentication for SSH via *pam_duo*
  - XSEDE customization of *pam_duo*
  - PSC customization of *pam_duo*
- Design of Authentication Decision Tree
- Implementation Example with Linux-PAM on PSC *Bridges*

PSC *Bridges*

- *Bridges* is an NSF-funded, 1.3PF HPC cluster designed and built by PSC to serve diverse computational applications, with an emphasis on large-shared-memory and GPU applications.
  - https://www.psc.edu/resources/computing/bridges


BRIDGES
A PITTSBURGH SUPERCOMPUTING CENTER RESOURCE
psc.edu/bridges
20 Storage Building Blocks, implementing the parallel *Pylon* filesystem (~10PB) using PSC's SLASH2 filesystem
4 MDS nodes
2 front-end nodes
2 boot nodes
8 management nodes
6 "core" Intel® OPA edge switches: fully interconnected, 2 links per switch
Intel® OPA cables
800 HPE Apollo 2000 (128 GB) compute nodes
4 HPE Integrity Superdome X (12TB) compute nodes ...
... each with 2 OPA↔IB gateway nodes
42 HPE ProLiant DL580 (3TB) compute nodes
12 HPE ProLiant DL380 database nodes
6 HPE ProLiant DL360 web server nodes
20 "leaf" Intel® OPA edge switches
32 RSM nodes with NVIDIA P100 GPUs
16 RSM nodes with NVIDIA K80 GPUs
Purpose-built Intel® Omni-Path topology for data-intensive HPC
Bridges Virtual Tour: http://staff.psc.edu/nystrom/bvt
This tool depicts the current plan for PSC's Bridges HPC system. Details are subject to change.

PSC *Bridges* is an XSEDE HPC Resource



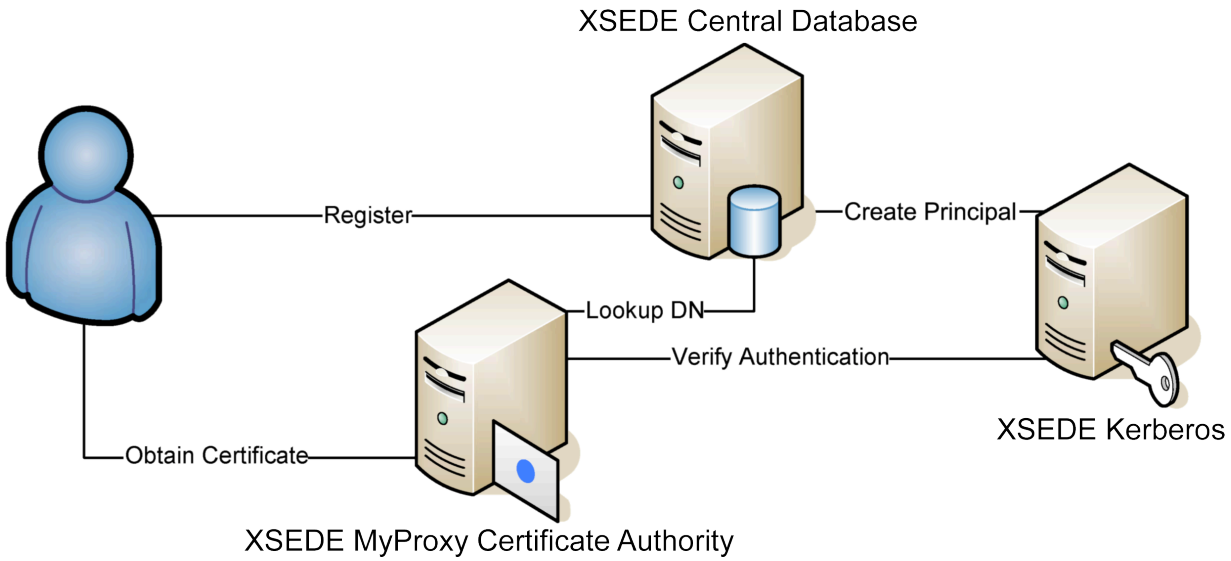
PSC PITTSBURGH SUPERCOMPUTING CENTER

SSH and GSI-OpenSSH

- Secure Shell (SSH) has been the de facto interactive login and data transfer service on Linux systems for over 20 years.
- GSI-OpenSSH is a customized edition of the popular OpenSSH implementation of SSH, developed by the National Center for Supercomputing Applications (NCSA).
- GSI-OpenSSH adds Globus Grid Security Infrastructure (GSI) authentication utilizing X.509 credentials and user mapping:
  - Users' X.509 certificate subjects (a.k.a. Distinguished Names, DNs) are mapped to their local username on the login host via a *grid-mapfile*
  - GSI-OpenSSH adds a configuration option, **PermitPAMUserChange**, which enables the current USERNAME value to be substituted during Linux-PAM processing

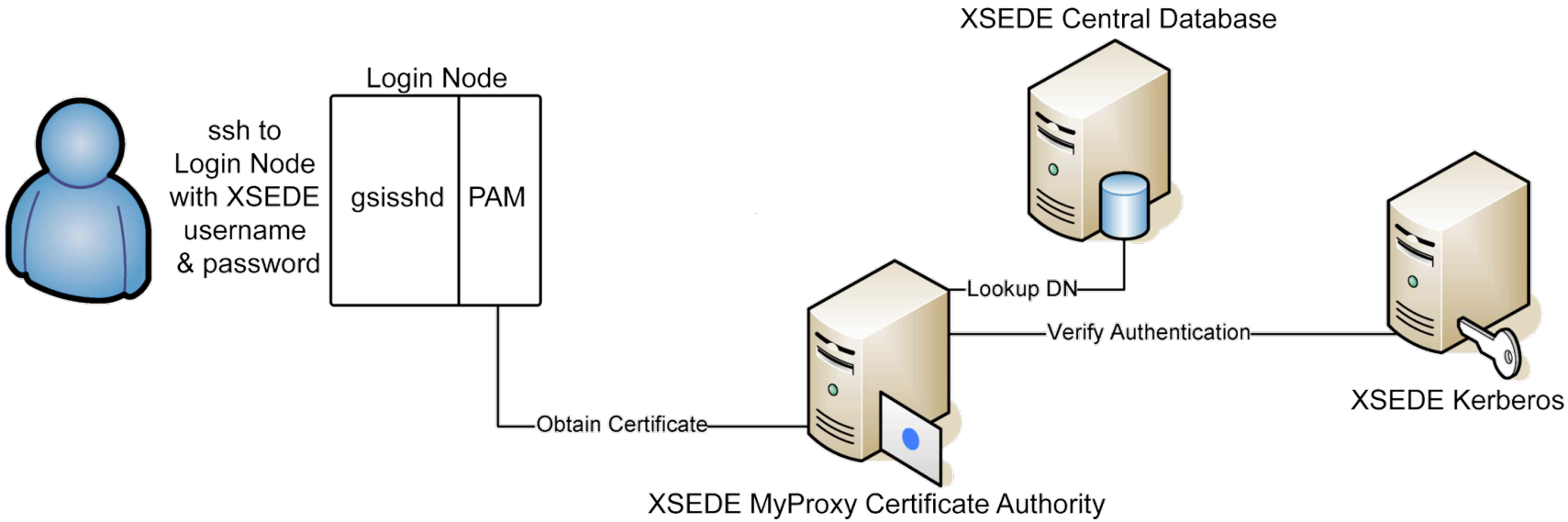
XSEDE Single Sign-On (SSO)

- To facilitate Single Sign-On across XSEDE resources, XSEDE Service Providers deploy Globus GSI-authenticated services, including GSI-OpenSSH and Globus GridFTP.
- To simplify issuance of X.509 user certificates, XSEDE operates a MyProxy Certificate Authority (CA) Service:



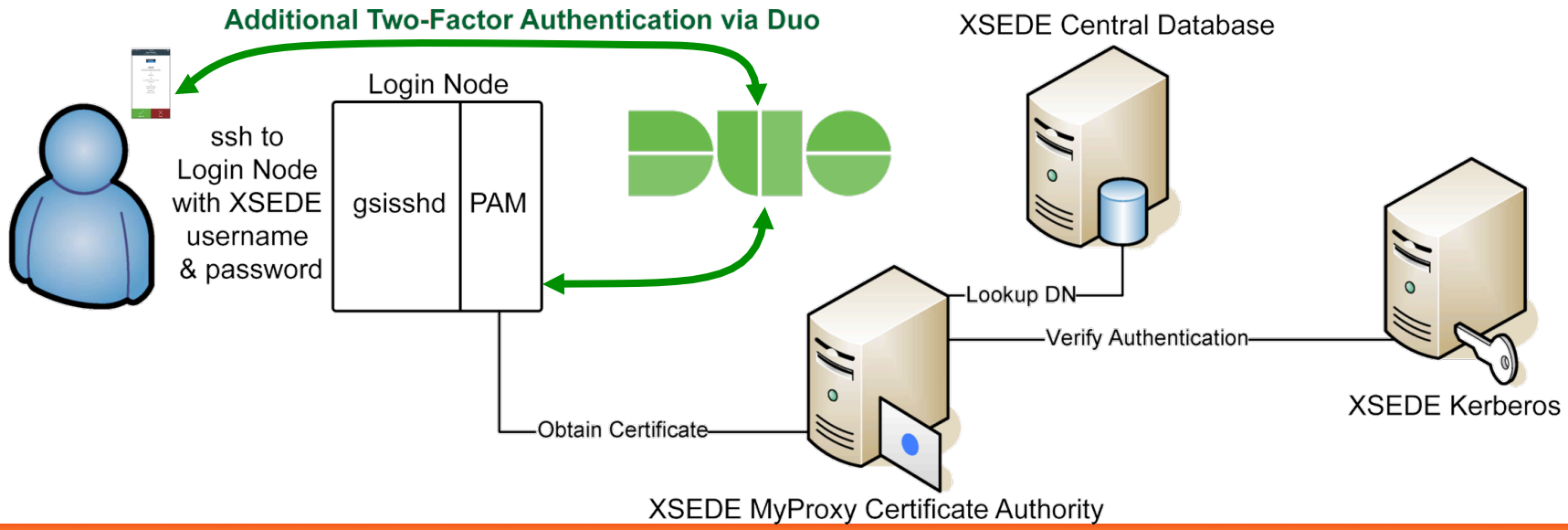
XSEDE-SSO with MyProxy-Enabled GSISSH

- To further simplify XSEDE SSO on login nodes, GSI-OpenSSH is deployed with Linux-PAM for authentication.
- Via PAM, a user certificate is automatically retrieved from the XSEDE MyProxy CA for the user, which is then used to map the user to their local account on the login node.



XSEDE SSO Login with *Duo* Two-Factor AuthN

- For stronger user authentication, XSEDE subscribes to the *Duo* two-factor authentication(TFA) service.
  - XSEDE users enroll in XSEDE *Duo* TFA via the XSEDE User Portal
- *Duo* provides a PAM module (pam_duo) to incorporate additional authentication into PAM-compatible services.



PSC PITTSBURGH SUPERCOMPUTING CENTER

Requirements for Flexible Multi-factor Authentication

- **Limited MFA Requirement**
  - Only specific users and groups of users are required to use MFA
- **Varying MFA Requirement**
  - The list of MFA-required users and MFA-required groups' membership will change over time
- **MFA Service Enrollment**
  - MFA-required users must enroll in the MFA service before authentication can succeed
- **MFA Integration Interface to SSH**
  - The MFA implementation should integrate with SSH via PAM
  - SSH-native authentication methods must not be able to bypass MFA
- **Mapping of Federated User Identity to Site-Local Identity**
  - The federated identity used to authenticate with the federated MFA service must be mapped to the correct corresponding local site identity to start a login session
- **Consistency of Enforcement**
  - All login methods, including additional SSH services on the target login node, must not allow the users and groups of users required to authenticate with MFA to bypass it.

XSEDE customization for *pam_duo*

- *pam_duo* normally checks to see that the user attempting to authenticate to Duo has an account of the same name on the local system. If not found, it returns PAM_USER_UNKNOWN.
- Users authenticating to XSEDE's Duo subscription do so using their federated XSEDE username.
- Since the user's local username on the login host may differ from their federated XSEDE username, this username check by *pam_duo* on the login host is not an appropriate check.
- XSEDE customized *pam_duo.c* to add a new *pam_duo* command-line parameter, **nosshpwcheck**, which when specified disables the local username check in *pam_duo*.

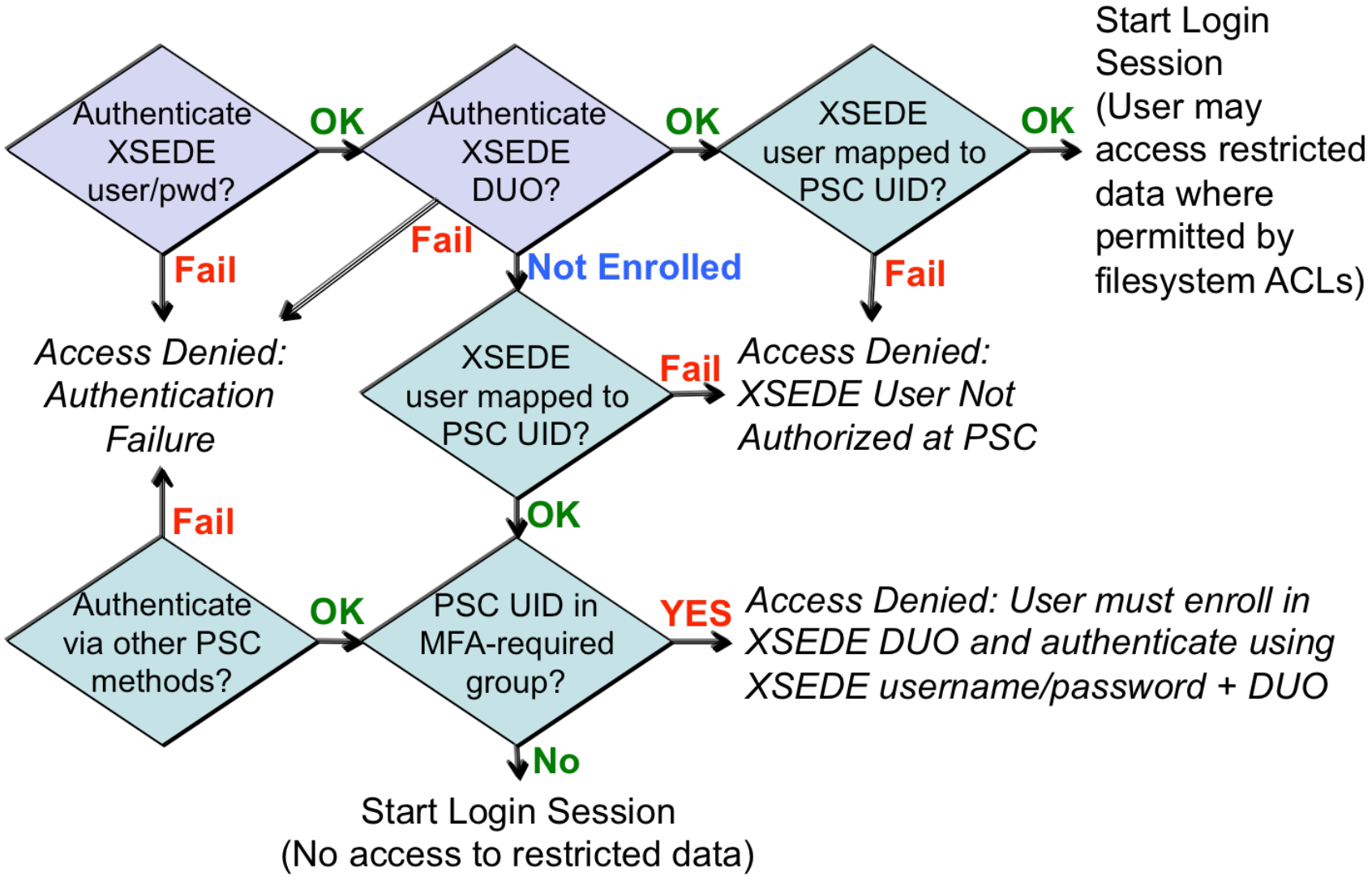
PSC customization (1) to *pam_duo*

- The Duo configuration file allows you to specify a *failmode* to control how a Duo client should respond if an attempt to authenticate using the Duo service fails for any reason.
- The default *failmode* specified in the source code is **DUO_FAIL_SAFE**, which means that if something goes wrong, DUO responds as if authentication succeeded, to prevent unintended lockout due to failed DUO authentication.
- If ACLs on the DUO configuration file are wrong, then it may not be read and default values will apply.
- PSC changed the default *failmode* value in *lib/util.c* to **DUO_FAIL_SECURE**, which denies authentication on failures.

PSC customization (2) to pam_duo

- If a user is not yet enrolled in a Duo service account, the pam_duo module returns PAM_SUCCESS by default.
- To enforce the requirement that MFA-required users must enroll in MFA before authentication can succeed, a new *pam_duo* command-line parameter, **enrolledreqd**, was added to tell *pam_duo* to return **PAM_AUTHINFO_UNAVAIL** if a user has not yet enrolled in the Duo service.
- To prevent duplication of *pam_duo* authentication in both the PAM **auth** and PAM **account** stacks, a means was needed to communicate Duo status between PAM stacks. A PAM environment variable, ***PAM_DUO_AUTHN***, was added to carry the return value of *pam_duo* so that it can be checked.

Design of Authentication Decision Tree



PSC PITTSBURGH SUPERCOMPUTING CENTER

Implementation Example on PSC Bridges

- /etc/pam.d/gsisshd
- /usr/xsede/etc/pam.d/xsede-tfa.auth
- /etc/pam.d/sshd
- /usr/xsede/etc/pam.d/xsede-tfa-check.acct

(Full details are provided in the PEARC17 paper)

- Sample output for denied users
- Sample output for an XSEDE Duo-authenticated user

Example: /etc/pam.d/gsisshd

```
[root@br006:~]# cat /etc/pam.d/gsisshd
#%PAM-1.0
auth       required     pam_sepermit.so
auth       include   /usr/xsede/etc/pam.d/xsede-tfa.auth
auth       include      password-auth
account    required     pam_nologin.so
account    include   /usr/xsede/etc/pam.d/xsede-tfa.acct
account    include      password-auth
password   include      password-auth
# pam_selinux.so close should be the first session rule
session    required     pam_selinux.so close
session    required     pam_loginuid.so
# pam_selinux.so open should only be followed by sessions to be executed
in the user context
session    required     pam_selinux.so open env_params
session    optional     pam_keyinit.so force revoke
session    include      password-auth
session   include   /usr/xsede/etc/pam.d/xsede-tfa.sess
```

Example: /usr/xsede/etc/pam.d/xsede-tfa.auth

```
[root@br006:~]# cat /usr/xsede/etc/pam.d/xsede-tfa.auth

auth  optional  pam_echo.so file=/usr/xsede/etc/xsede-tfa-msg.txt

auth  [success=ok new_authtok_reqd=ok default=die]  /usr/xsede/lib64/security/pam_remapuser.so /usr/
xsede/sbin/auth_myproxy_user.sh

auth  [success=ok new_authtok_reqd=ok authinfo_unavail=1 service_err=die default=die]   /usr/xsede/
lib64/security/pam_duo.so conf=/usr/xsede/etc/duo/pam_duo-xsede.conf nosshpwcheck enrolledreqd debug

auth  sufficient  /usr/xsede/lib64/security/pam_remapuser.so /usr/xsede/sbin/auth_map_xsede_user.sh

# Do the following if the user was not enrolled in DUO (and deny access if they are required to be
enrolled).

auth  requisite  /usr/xsede/lib64/security/pam_remapuser.so /usr/xsede/sbin/auth_map_xsede_user.sh

auth  [success=ok auth_err=2 default=bad] pam_listfile.so onerr=succeed item=group sense=deny file=/
usr/xsede/etc/duo-required-groups

auth  [success=done auth_err=bad default=bad] pam_listfile.so onerr=succeed item=user sense=deny
file=/usr/xsede/etc/duo-required-users

auth  [default=1] pam_echo.so file=/usr/xsede/etc/denied-user-msg.txt

auth  optional    pam_echo.so file=/usr/xsede/etc/denied-group-msg.txt

auth  optional    pam_echo.so file=/usr/xsede/etc/xsede-duo-enroll-msg.txt

auth  requisite   pam_deny.so
```

Example: /etc/pam.d/sshd

```
[root@br006:~]# cat /etc/pam.d/sshd
#%PAM-1.0
auth       required     pam_sepermit.so
auth       substack     password-auth
auth       include      postlogin
# Used with polkit to reauthorize users in remote sessions
-auth      optional     pam_reauthorize.so prepare
account    required     pam_nologin.so
account    include  /usr/xsede/etc/pam.d/xsede-tfa-check.acct
account    include      password-auth
password   include      password-auth
# pam_selinux.so close should be the first session rule
session    required     pam_selinux.so close
...
```

Example: /usr/xsede/etc/pam.d/xsede-tfa-check.acct

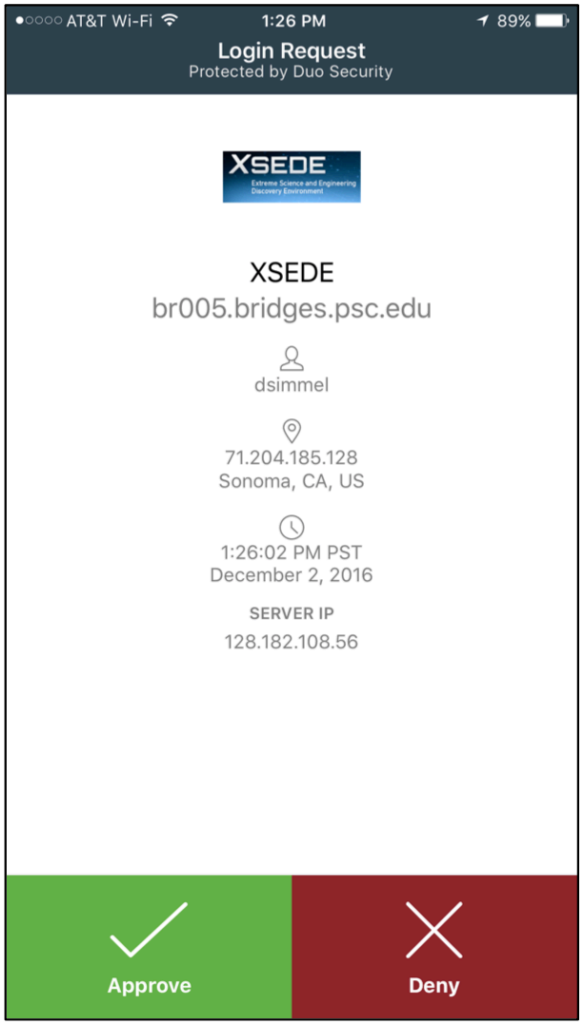
```
[root@br006:~]# cat /usr/xsede/etc/pam.d/xsede-tfa-check.acct
account [success=ok auth_err=2 default=bad] pam_listfile.so onerr=succeed
item=group sense=deny file=/usr/xsede/etc/duo-required-groups

account [success=4 auth_err=bad default=bad] pam_listfile.so onerr=succeed
item=user sense=deny file=/usr/xsede/etc/duo-required-users

account [default=1] pam_echo.so file=/usr/xsede/etc/denied-user-msg.txt

account optional    pam_echo.so file=/usr/xsede/etc/denied-group-msg.txt

account optional    pam_echo.so file=/usr/xsede/etc/xsede-duo-reqd-msg.txt

account requisite   pam_deny.so
```

Sample output for denied users

```
$ ssh joeuser@bridges.psc.xsede.org

Access denied: user
XSEDE DUO authentication is required for login access to
this system. SSH publickey and gsissh authentication are
not permitted when XSEDE DUO is required.
For additional help, send e-mail to help@xsede.org.
Connection closed by 128.182.108.56


$ ssh -p 2222 -l joeXsede bridges.psc.xsede.org

XSEDE Authentication
password:

Access denied: group
XSEDE DUO authentication is required for login access to
this system. Please log in to the XSEDE User Portal and
enroll in DUO under My XSEDE->Profile:
https://portal.xsede.org/group/xup/profile#/
For additional help, send e-mail to help@xsede.org.
```

Sample output for an XSEDE Duo-authenticated user

```
$ ssh -p 2222 -l joeXsede bridges.psc.xsede.org

XSEDE Authentication
password:

Duo two-factor login for joeXsede

Enter a passcode or select one of the following options:

 1. Duo Push to XXX-XXX-1234
 2. Phone call to XXX-XXX-1234

Passcode or option (1-2): 1

Pushed a login request to your device...
Success. Logging you in...

Last login: Thu Jun  8 16:59:12 2017 from example.psc.edu

****************** W A R N I N G ********************
You have connected to br006.pvt.bridges.psc.edu

This computing resource is the property of the Pittsburgh
Supercomputing Center. It is for authorized use only.  By
using this system, all users acknowledge notice of, and
agree to comply with, PSC polices including the Resource
Use Policy, available at
http://www.psc.edu/index.php/policies. Unauthorized or
improper use of this system may result in administrative
disciplinary action, civil charges/criminal penalties,
and/or other sanctions as set forth in PSC policies. By
continuing to use this system you indicate your awareness
of and consent to these terms and conditions of use.

LOG OFF IMMEDIATELY if you do not agree to the conditions
stated in this warning

Please contact remarks@psc.edu with any comments/concerns.

****************** W A R N I N G ********************

[joeuser@br005:~]$
```



PSC
PITTSBURGH SUPERCOMPUTING CENTER

Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant No. ACI-1445606, *"Bridges: From Communities and Data to Workflows and Insight"* and Grant No. ACI-1548562, *"XSEDE 2.0: Integrating, Enabling and Enhancing National Cyberinfrastructure with Expanding Community Involvement."*

We would like to acknowledge the contributions made by Venkatesh Sri Yekkirala at NCSA for his XSEDE-sponsored efforts to enable the use of federated identities with Duo multi-factor authentication.

References (1)

- PEARC17 paper available in ACM Digital Library at:
  - https://doi.org/10.1145/3093338.3093392
- PEARC17 paper and pam_duo patches available at:
  - https://github.com/pscedu/duo_unix_psc
- Instructions for applying the patches to the duo_unix source
  - https://github.com/pscedu/duo_unix_psc/wiki
- Linux Pluggable Authentication Modules (Linux-PAM)
  - http://www.linux-pam.org
  - Note that the Offline documentation is more current than the online HTML editions; download the document tar.gz archive that matches your release.
- *pamtester* utility
  - http://pamtester.sourceforge.net
  - Available for installation using yum in EPEL repo

References (2)

- OpenSSH
  - http://www.openssh.com
- GSI-Enabled OpenSSH (GSI-OpenSSH)
  - http://grid.ncsa.illinois.edu/ssh/
- PSC High-Performance Networking patches for OpenSSH (HPN-SSH)
  - https://github.com/rapier1/openssh-portable
- MyProxy Credential Management Service
  - http://grid.ncsa.illinois.edu/myproxy/
- XSEDE MyProxy-Enabled GSISSH (part of the xsede-user-tfa-ssh package)
  - https://software.xsede.org/development/xsede-user-tfa-ssh/
- Duo Unix – Two-Factor Authentication for SSH with PAM support
  - https://duo.com/docs/duounix