XSEDE Central Services Baseline Security Standard

October 3, 2013

Version 1.1

Table of Contents

A. Document History

Relevant Sections	Version	Date	Changes	Author
Entire Document	1.1	10/3/2013	Baseline	A. Slagell

B. Document Scope

Through acceptance of the XSEDE Level 1 SP Security Agreement and other contracts, providers of XSEDE central services agree to follow this security baseline document approved by the XSEDE Security Working Group (XSWoG). Because of the natural trust relationships between major XSEDE resources and the interdependence of them, security vulnerabilities affect far more than a single service provider. Therefore, this document sets forth minimum, security standards for providers of central services whose compromise could have a direct impact upon XSEDE. The list of security controls comes both from inherited practices of TeraGrid and new findings in the XSEDE risk assessment.

C. Document Body

C.1. Introduction

Through acceptance of the XSEDE Level 1 SP Security Agreement and other contracts, providers of XSEDE central services agree to follow this security baseline document approved by the XSEDE Security Working Group (XSWoG). Because of the natural trust relationships between major XSEDE resources and the interdependence of them, security vulnerabilities affect far more than a single service provider. Therefore, this document sets forth minimum, security standards for providers of central services whose compromise could have a direct impact upon XSEDE. The list of security controls comes both from inherited practices of TeraGrid and new findings in the XSEDE risk assessment.

C.2. Definitions

XSEDE Central Service: These are XSEDE services, usually supported by a Level 1 Service Provider, which XSEDE users depend upon either directly or indirectly and whose integrity and availability affect more than a single service provider. While many of these are exclusive to XSEDE (e.g, XCDB, AMIE, and the XSEDE Kerberos realm) some serve other customers as well, such as, GlobusOnline. The Systems Operational Support group maintains the official list of XSEDE central services.

C.3. Security Baseline Standards

Items in this section are standards to establish a minimum baseline, i.e., part of the expectations for each central service provided. At the end of the document, we have additional guidelines recommended for service providers to apply as best makes sense for their environments.

C.3.1. Vulnerability Management

Most security incidents target existing vulnerabilities that have long since had remedies available. One of the most effective activities to reduce exposure and prevent incidents is to maintain up-to-date and properly patched software. This is true both for users at home, and those running entire data centers.

Therefore, providers of XSEDE central services are expected to:

- To maintain software patches such that they are up-to-date against *exploitable* vulnerabilities (for which there is a remedy) considered a *significant threat* to XSEDE. This is for all XSEDE resources as well as those with special trust relationships and dependencies with XSEDE resources (e.g., not just an HPC for XSEDE resources, but also the authentication server that it depends upon).
- Be able to identify systems vulnerable to a particular exploit, and report back plans for risk mitigation.

- Perform regular (at least weekly) scanning for unmitigated vulnerabilities. XSEDE will provide use of the Qualys scanner for those wishing to use it.

- Test that vulnerabilities are not reintroduced after configuration changes. For this a configuration management tool, such as, Puppet or cfEngine is recommended.

C.3.2. Authentication & Authorization

It is critical to control access to XSEDE resources, especially in cases of privileged access. It is equally important to accurately record who has access to systems and that they are not exceeding their authority. Therefore, providers of XSEDE central services are expected to:

- Use strong, i.e., at least two-factor, authentication for administrative interfaces, accounts or privilege escalation where at all possible. This could be directly on a system or through use of a choke point such as a bastion host or VPN.

- Eliminate the use of local passwords where possible.

- Disable plaintext authentication over the network.

- Record audit logs of all authentication attempts, including privilege escalations.

- Maintain and audit the list of admins and privileged users to avoid authorization creep and to remove access when employees leave or roles change.

- Notify the XSWoG of any SP security staff changes that would require revoking, granting or modifying access to XSWoG resources (secure jabber/wiki, mailing lists, hotline, etc.[1])

C.3.3. Audit Logging

It is critical to maintain the integrity of system and network logs in order to investigate security incidents. As such, the *XSEDE Level 1 SP Security Agreement* states that service providers will maintain the logs necessary for incident investigation for at least 90 days. This holds for all central services. In the section above, it is also noted that records of attempted access are a part of these logs that must be recorded. Because it is trivial for an adversary who has compromised a server and gained root to erase his tracks in the logs, service providers are expected to copy these audited events to an external log server for safe-keeping—for example, using syslog-ng to connect to a hardened, remote log host.

C.3.4. Network Monitoring

System and authentication logs are very important but often not sufficient to investigate all security incidents. Equally important are networks logs. While providers of XSEDE central services are not

[1] https://ops-security.xsede.org/wiki/Checklist_for_Departing_Security_Staff

necessarily expected to run a full Intrusion Detection/Prevention System, which can be very costly, they do need to maintain NetFlow level logs and statistics at their borders, particularly those for XSEDENet. A service provider is expected to be able to answer if they have seen activity from specific IP addresses within a particular range of time.

C.3.5. Auditing

As configuration changes can accumulate over time, systems and services can drift from baselines. Therefore, it is expected that service providers audit themselves for compliance with this baseline at least annually and to report on the results.

C.3.6. Physical Access

XSEDE systems and services are not to be placed in public or unrestricted areas. They must be secured in a facility that has a way to audit who has access to rooms with these systems and preferably audit logs to confirm who has had access at a given time. If the latter is not possible, they need to physically restrict access to racks with XSEDE servers to a minimal list of employees. If outsourcing hosting to external providers such as Amazon, they must require that their external service provider has physical controls no lower than their own.

C.4. Additional Guidelines

The above list of items is not exhaustive of all that one must do to be following security best practices within this industry, but instead it is a minimum list of items for a baseline that sites can all agree upon. There are many other useful security controls, some of which we present below.

C.4.1. Host Security

The following recommendations are made to protect XSEDE systems and services at the host level.

- **Disable or remove unneeded services and accounts.** Often these will be installed by default by operating systems or software.
- **Eliminate unnecessary setuid/setgid bits on executables.** If unneeded, these should be removed as they can be used for privilege escalation attacks.
- **Filter source IPs connecting to critical or administrative services.** TCPWrappers, host-based firewalls and router ACLs are all useful to restrict access to certain interfaces or IP addresses. This is most practical and most useful for administrative interfaces with a small set of users, but can sometimes be used effectively more broadly. Often one can create a single choke point to several administrative services through a hardened bastion host or VPN
- **Use minimal permissions for exporting NFS shares.** NFS shares should only be exported locally and not across trust boundaries. Furthermore, minimal permissions

should be used for a given scenario. There are several built-in restrictions available, such as, nosuid, root_squash, noexec, nodev and read-only exports.

- **Use a host-based IDS for integrity checking and log monitoring**. Host-based IDSs, such as OSSEC, provide many capabilities. Two very important ones are file *integrity checking*, to detect modified configurations or binaries, and *log monitoring*, which can watch for security events and correlate across log sources.

- **Use TLS/SSL or other network encryption technologies where possible, especially if crossing system boundaries**. Most authenticated services support versions that use SSL or a similar technology to provide authenticity, integrity and confidentiality. In other cases, it is often possible to add-on encryption with tools like stunnel or SSH.

- **Monitor command line history with process accounting or an instrumented SSHD.** It is all too easy for an adversary to clean out shell history or stop recording it, but this is one of the most useful sources of forensic information. Process accounting or specially instrumented SSH daemons can overcome this problem and record that information, even though it would be unavailable to the network IDS due to encryption.

- **Use a centralized logging infrastructure.** As already noted, it is important to log to a remote host to protect the integrity of the logs. More than that, it is useful to send as many of the logs as possible to the same place for alert correlation and greater visibility. These log servers should also be backed up, incase they too are the target of an attack.

C.4.2. Network Security

The following are recommended to protect XSEDE resources at the network level.

- **Use egress/ingress filters to protect against spoofing.** Because of the trusted relationship between sites, it is especially important not to let your network be used to spoof traffic.

- **Disable source routing at trust boundaries.** This technology can be abused for man-in-the-middle attacks.

- **Utilize firewalls and ACLs as appropriate.** These are often more robust than host-based firewalls and can be used in conjunction with other controls for layered security.

- **Deploy a network IDS to monitor for attacks against and emanating from your networks.** IDSs are by no means a panacea, but they can be an important piece of the overall site security architecture.