

TeraGrid Security Working Group Newbie Guide and FAQ

Status: DRAFT

This document is a draft for discussion. A number of editorial changes have been made to this revision, including:

1. Renumbering of sections and creation of table of contents
2. Additional sections: Status, Abstract, Acknowledgements, Security Statement, Editor information, references
3. Changed references to the TeraGrid Executive Committee (previous, construction project) to either TeraGrid Director or TeraGrid Security Officer as appropriate (new management structure as of August 2005)
4. Formalized references
5. Added information on the incident@teragrid.org mailing list and detailed the purpose of it and the "Incident-announce@teragrid.org" mailing lists.

Abstract

The TeraGrid is a large, distributed enterprise with complex procedures and policies. This guide is intended to assist new security personnel who are joining the TeraGrid security community. It is useful both for new staff at existing sites and for staff from new sites.

Table of Contents

1. The TeraGrid Security Working Group	3
1.1 What is the TeraGrid Security-WG?	3
1.2 How do I contact Security-WG members?	3
1.3 What do I do in case of a security emergency?	3
1.4 Typical Security-WG Topics and Tasks	3
1.5 Mailing lists	4
1.6 Teleconferences	4
2. Security-WG Resources	4
2.1 Repo	4
2.2 TeraGrid Security-WG secure site	5
3. TeraGrid Security (New site guide)	5
3.1 Basic expectations	5
3.2 Certificate Authorities	5
3.3 Risk Assessments	5
4. General	5
4.1 Generating documents	5
4.2 Email encryption	5
5. TeraGrid Specific Software Systems	6
5.1 AMIE (Account Management Information Exchange)	6
5.2 Inca	6
6. Security Considerations	6
7. Acknowledgements	6
8. Author Information	6

DRAFT
Security Working Group

Jim Marsteller (PSC)
October 4, 2005
Editorial Revisions (Charlie Catlett, UC/ANL)
February 7, 2006

9. References 6

1. The TeraGrid Security Working Group

1.1 What is the TeraGrid Security-WG?

The following description is adapted from the Security Working Group Charter [1]:

The TeraGrid Security Working Group reviews security policy and security-related implementation issues to make recommendations to the TeraGrid Security Officer and TeraGrid Director regarding security policies and practices that should be adopted by TeraGrid member sites and users. The participants of the TeraGrid Security-WG DO NOT constitute the information security incident response staff for the TeraGrid.

Because even a small design change can dramatically effect the overall security of a system, the TeraGrid Security Officer will consult the Security-WG regarding modifications to the TG operation for possible security implications prior to any implementation. The Security-WG will work with each of the other TeraGrid working groups to review and address security implications of software, services, and policies developed in those working groups. Where possible, the Security-WG will maintain a liaison to each of the other TeraGrid working groups.

1.2 How do I contact Security-WG members?

Contact information can be found in the security section of the TeraGrid Repository ("Repo" - repo.teragrid.org, see §2.1) in the drafts directory as "teragridemercontact" available as both a MS-Word document and as a PDF.

Security-WG Chair email: (security-lead@teragrid.org).

1.3 What do I do in case of a security emergency?

Emergency contacts are available in Repo (see §2.1). Relevant documents are:

teragridemercontact.pdf/.doc for emergency individual contacts.

There is a hotline that can be used 24 hours a day. This number is known to each site's Security Working Group lead. New sites should contact the Security-WG chair or TeraGrid Security Officer for this information.

1.4 Typical Security-WG Topics and Tasks

The Security-WG focuses on a broad range of coordination, response, and planning efforts. Ongoing work involves policy and procedure development as well as coordinating emergency incident response.

Typical projects coordinated by the Security-WG include pilot projects (e.g. Kerberos, Science Gateway authorization schemes, etc.) as well as general processes such as review of Certificate Authorities and conducting risk assessment exercises.

Documents that have been drafted to date by the Security-WG include:

Security Baselines
Incident Report and Incident Flowchart

Playbook
TeraGrid Site Security Memorandum of Understanding (MOU)

1.5 Mailing lists

TeraGrid Security-WG (security-wg@teragrid.org)

To become a member of the TeraGrid Security-WG, you must be a security representative from a TeraGrid site. To request to be added to the mailing list, send email to the Security-WG lead.

Incidents Announce (incident-announce@teragrid.org)

The primary purpose for this list is to announce Incident Response meeting details and share “non-critical” Incident Response information with the TeraGrid Incident Response team.

To be added to the incidents announce list, Security-WG members may send requests to the Security-WG lead.

Incident (incident@teragrid.org)

This list is used to communicate critical security event information that requires immediate attention of the TeraGrid Incident response team. Because mail sent to this list may trigger emergency notification and escalation action, it should only be used for Security emergencies that directly affect the TeraGrid project. Subscription to this list is determined by the Incident Response contact per site as detailed in the TeraGrid Security Contact List document found in the security section of the TeraGrid Repository (“Repo” - repo.teragrid.org, see §2.1)

Security-WG Chair (security-lead@teragrid.org)

Email will be sent to the Security-WG Chair and the Network, Operations and Security Area Director.

TeraGrid Working Group (wg@teragrid.org)

This list is a TeraGrid-wide broadcast list that includes all members of all TeraGrid mailing lists.

Others

Numerous other mailing lists exist for the other working groups. Details can be found by inquiring with representatives of those groups.

1.6 Teleconferences

TeraGrid Security-WG call

Currently, a bi-weekly call is used for coordination and communication, with participation expected from all members of the TeraGrid Security Working Group. Future plans, current issues, and security issues are discussed during these calls. Please contact the Security-WG lead for the phone number and scheduling information (security-lead@teragrid.org).

Weekly incident response call

Currently, a weekly call for site incident responders is used to review current security incidents and emerging threats. Discussion of tools, vulnerabilities, and detection methods are typical.

2. Security-WG Resources

2.1 Repo

Repo is the working TeraGrid repository for documents and data. TeraGrid participants can request access to Repo by emailing help@teragrid.org. Repo can be accessed at:

<http://repo.teragrid.org>

Security documents are available at: <http://repo.teragrid.org/head/security>

2.2 TeraGrid Security-WG secure site

The Security-WG uses a secure site for event documentation. Information about this site is provided to incident handlers from the Security-WG as needed.

3. TeraGrid Security (New site guide)

3.1 Basic expectations

New sites are expected to participate in the TeraGrid Security-WG, and to make appropriate security and emergency contact informational available for inclusion in the Security-WG contact lists. Additional responsibilities include those outlined in the following documents:

- TeraGrid Baseline Security Requirements [2]
- TeraGrid Security Memorandum of Understanding [3]
- TeraGrid Certificate Management and Authorization Policy [4]

Security staff should also be aware of:

- TeraGrid Security-WG Recommendations for Best Practices [5]

3.2 Certificate Authorities

Sites wishing to add an existing CA to the TeraGrid must meet the requirements outlined in [4]

Sites and users are also expected to comply [4].

3.3 Risk Assessments

Sites are expected to participate in an annual risk assessment process. Data gathered during the risk assessment is typically generalized, and is considered private.

4. General

4.1 Generating documents

When creating documents for use in the Security-WG, please provide an editable version (TXT, RTF, or DOC) as well as a non-proprietary format (TXT or PDF) of the document.

4.2 Email encryption

Sensitive email sent to the Security-WG or the Incidents list must be encrypted using PGP/GPG. Details can be obtained from the Security-WG lead.

Email to individual Security-WG members may be encrypted using their PGP keys. Keys are regularly exchanged and signed at Security-WG meetings and can also be obtained from key repositories with proper verification.

5. TeraGrid Specific Software Systems

5.1 AMIE (Account Management Information Exchange)

AMIE is an identity and accounting data management and transfer system used by the TeraGrid to replicate, update, and propagate accounts and accounting data. A security analysis of AMIE has been done and can be found in [6].

AMIE is typically implemented using a restricted, unprivileged account. The AMIE software itself has not been reviewed for security by TeraGrid staff.

5.2 Inca

Inca is a flexible framework for the automated testing, benchmarking and monitoring of Grid systems. It includes mechanisms to schedule the execution of information gathering scripts, and to collect, archive, publish, and display data. More information on Inca can be found at: <https://repo.teragrid.org/inca/>

The INCA software itself has not been reviewed for security by TeraGrid staff.

6. Security Considerations

As this document outlines procedures and processes related to the Security-WG and general TeraGrid security activities. The security impact of the processes outlined in this document relates to information security with respect to communication among TeraGrid Security staff. The consequences of poorly designed or implemented security coordination and communication include ineffective response to security threats and events as well as reduced security posture for the TeraGrid project.

7. Acknowledgements

This work was supported by the National Science Foundation grant numbers ACI-0122296, "Distributed Terascale Facility: Build and Extend the DTF," and ACI-0307136, "TCS and ETF Operations."

8. Author Information

Jim Marsteller <jam@psc.edu>
Pittsburgh Supercomputing Center
4400 Fifth Avenue
Pittsburgh, PA 15213
(412) 268-4960
(412) 268-5832 (Fax)

9. References

- [1] Security-WG Charter, 1.0
<https://repo.teragrid.org/head/security/TG-Security-WG-Charter-1.0.txt>
- [2] TeraGrid Baseline Security Requirements

- https://repo.teragrid.org/head/security/Policy_Procedures/tg-baseline.pdf
- [3] TeraGrid Security Memorandum of Understanding
https://repo.teragrid.org/head/security/Policy_Procedures/Security-MOU.pdf
- [4] TeraGrid Certificate Management and Authorization Policy, D. Simmel, ed. July 2004.
https://repo.teragrid.org/head/security/Policy_Procedures/CertMgmtAuthPolicy.pdf
- [5] TeraGrid Security-WG Recommendations for Best Practices
<https://repo.teragrid.org/head/security/drafts/security-practises.txt>
- [6] AMIE Account Security Evaluation, J. Basney, February 2004.
<https://repo.teragrid.org/head/account-management/doc/AMIE/>
(document name "AccountSecurityEvaluation.txt" at this URL)