Overview of the U.S. ATLAS Computing Facilities

Cyber Security Plan

November 2012

Abstract

This document provides a brief overview of computing security for the ATLAS collaboration in the United States (U.S. ATLAS). It refers to comprehensive security plans and other documentation created by organizations offering computing and middleware services to the collaboration, and it provides a description of the context in which those plans are applied.

Introduction and Context

The ATLAS collaboration maintains a distributed computing facility consisting of the Tier-1 at Brookhaven National Laboratory (BNL), five Tier-2 sites (which in all but one cases consist of multiple institutions), and numerous Tier-3 sites. This document provides an overview of the computing security plan for the distributed facilities.

Typically an organization's computing security plan contains explicit assessments, policies, procedures, and controls, all created for and by that single organization. In the case of US ATLAS, the computing activities take place within a framework of multiple, overlapping security regimes, deriving from several organizations the U.S. ATLAS Facilities are part of. Instead of explicitly listing security policies, the role of the facilities in the relevant organizations is explained, and reference to their respective security plan documentation is made.

The organizations relevant to US ATLAS security are:

- Each U.S. ATLAS site complies with any relevant local site security requirements imposed by the organization hosting the site.
- Each U.S. ATLAS site is a participant in Open Science Grid (OSG) and complies with OSG’s security plan.
- As a subset of the ATLAS virtual organization (VO), all U.S. ATLAS sites are participants in the Worldwide LHC Computing Grid (WLCG), and they comply with WLCG's security guidelines.
- As a subset of the global ATLAS VO, U.S. ATLAS has contacts and interactions with the European Grid Infrastructure (EGI) which has its own grid-level security plan that U.S. ATLAS must remain consistent with
- ATLAS has security policies purely at the VO level driven by collaboration-internal requirements, and the U.S. ATLAS Facilities follow them.
- U.S. ATLAS sites have implicit, security-related relationships with several other entities which shall be mentioned even where they do not impose direct requirements.

Institutional and Facility Site Plans

None of the sites making up the U.S. ATLAS Facilities are on their own. They all reside at institutions (universities or national laboratories) which impose their own computer security standards, policies, and procedures. In some cases these standards are relatively informal, while others impose restrictions/requirements that exceed what OSG/WLCG or the VO would otherwise follow.

For example, in the case of Brookhaven National Laboratory and Stanford Linear Accelerator (Tier-1 and Tier-2 respectively), those sites must follow Department of Energy security policies, and have formal facility security plans that document their compliance. These restrictions may include large arrays of system management requirements, special controls, network registration, and firewalls.

Other sites, especially institutional analysis facilities (Tier-3s) at universities, may have no local requirements beyond signing a campus end-user acceptable use agreement. Systems at these kinds of institutions are essentially directly internet-connected with no institution-driven system restrictions, nor any protection from outside attacks.

If a U.S. ATLAS facility site falls under a local institutional site plan, then that constitutes a minimum standard. Wherever a site standard differs from an ATLAS, WLCG, or OSG standard, the site will comply with the most restrictive. A survey of the full range of site plans in force at U.S. ATLAS sites is well beyond the scope of this document. Access to the details of such plans are typically limited or even tightly restricted. If additional details of site plans are required, it may be possible to get permission to share them with a limited audience.

Open Science Grid Security

- ATLAS' primary distributed computing security framework is that of the Open Science Grid (OSG). All U.S. ATLAS facilities are installed and maintained as OSG grid sites, using OSG-packaged software.

OSG has a fully developed and documented security plan, comparable to that of other large institutions and companies. Security is a top-level administrative area in OSG, led by the OSG security officer.

- Fully documented and defined VO user registration policy and procedures: These govern what steps the VO is obligated to do to verify users' identities and manage the user membership lifecycle.
- Explicitly defined risk assessment procedures: OSG security policies are developed from a well-defined methodology for assessing risk, recommending controls, and mitigating residual risks.
- Explicitly defined and documented organizational roles and responsibilities within OSG and between OSG and others (sites, VOs, users, software developers).
- Explicitly documented trust relationships and hierarchies.
- Privacy and acceptable use policies.
- End-user and admin education.
- Comprehensive incident response plan (also defining incident notification policies and procedures), along with periodic security challenges to exercise OSG's, sites' and VO's ability to respond to a security event.

Since OSG is simultaneously a software provider and a service provider, they also have facility- oriented security plans for the Grid Operations Center (GOC) providing those services.

In addition to being a national grid infrastructure organization, OSG is also taking on the role of primary Certificate Authority for the infrastructure in the U.S.

The OSG Security Plan is available at
http://osg-docdb.opensciencegrid.org/0003/000389/019/OSGSecurityPlanV5.pdf

Other OSG security documentation is available at http://osg-docdb.opensciencegrid.org/cgi-bin/ListBy?topicid=7

European Grid Infrastructure Security

The European Grid Infrastructure (EGI) is the European counterpart to OSG. U.S. ATLAS does not use EGI middleware at its sites, but the facilities do rely directly on global/central services provided by sites using the EGI middleware stack. U.S. ATLAS and OSG also rely on software developed under the auspices of the European grid organizations. Furthermore, since ATLAS' workload management systems are global, vulnerabilities or compromises that occur at EGI sites may involve credentials also used in the U.S.

Like OSG, EGI (formerly EGEE) has a well-developed and formal computing security plan, addressing a similar range of topics and concerns.

EGI security documentation is available at:

https://documents.egi.eu/public/ListBy?topicid =33 https://wiki.egi.eu/wiki/SPG:Documents

Incident response is coordinated through the EGI Cyber Security Incident Response Team (CSIRT).

https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page

Of particular interest to ATLAS, therefore also applicable to U.S. ATLAS, are policies regarding multi-job pilot frameworks, since PanDA, ATLAS' global workload management system, uses an overlay mechanism.

WLCG has adopted the EGI multi-job pilot policy which is documented at:

https://documents.egi.eu/public/RetrieveFile?docid=84&version=6&filename=EGI-SPG- PilotJobs-V1_0.pdf

Worldwide LHC Grid Security

The worldwide LHC Computing Grid (WLCG) is a cross-cutting organization created to coordinate the global distributed computing activities of the four LHC experiments (ALICE, ATLAS, CMS and LHCb).

WLCG itself also has security policies, with which the LHC VO sites and users are expected to comply with regardless of which Grid flavor they are working on. Their respective cyber security related directives refer to EGI and OSG policies and procedures, or set very reasonable best-practice standards similar to those set by other grids. For example, incidents are reported through the local site, with inter-grid security response handled between the EGI CSIRT and the OSG security team as the incident report moves up the hierarchy.

A comprehensive list of related documents is available at:

http://wlcg.web.cern.ch/security/computer-security

There is also a Technical Evolution Group dedicated to security

https://twiki.cern.ch/twiki/bin/view/LCG/WLCGSecurityTEG

ATLAS VO Security

ATLAS itself has a security team. For the most part, ATLAS VO security falls under the CERN-based IT infrastructure or under the WLCG security groups and efforts referred to above. The VO-specific aspects focus on things like promoting best coding practices among ATLAS developers, and ensuring that the ATLAS workload management system complies with the grid-level security plans.

Other Trust and Security Relationships

International Grid Trust Forum (IGTF) and Certificate Authorities (CA)

At this point most critical distributed authentication mechanisms used by U.S. ATLAS are based on the X.509 Public Key Infrastructure (PKI).

The usefulness of this infrastructure is based on the trust given to the Certificate Authorities (CAs) which issue end user and host credentials used for mutual authentication. The International Grid Trust Forum is the body which accredits the various Certificate Authorities and vouch for their internal policies and procedures. OSG and EGI trust the IGTF to vouch for the CAs, and the IGTF must trust the CAs to comply with their agreements.

To the extent that ATLAS relies on this infrastructure, all of their policies and procedures are part of ATLAS' security documentation.

Software Developers

Very little of the software used to implement the U.S. ATLAS facilities and the applications is written by the organizations defining the security plans discussed here. EGI and OSG (and ATLAS) package and distribute software written by a very large number of external developers. This software includes grid middleware, batch systems, as well as the open source operating systems that underpin the grids. From a security standpoint, both the Grid organizations, and the ATLAS VO must trust that those developers are providing software written in accordance with valid cyber security policies, guidelines and best practices.

Incident Reporting

Incident reporting provides a concrete case that illustrates the security relationships of U.S. ATLAS. All U.S. ATLAS resources and services are hosted at some site. That site is obligated to report any instance of a compromise to the OSG security team. Typically sites are also obligated to inform their institutional cyber security group (this is mandatory at DOE national laboratories and many universities). In the case of the national laboratories, this results in incident reports being passed on to the Department of Energy's cyber security organization.

The OSG Security team follows the incident response procedures as documented. Part of this procedure is to assess whether the problem has a global impact. If the nature of the incident suggests that it may have effects or causes beyond OSG, the OSG security team informs representatives of other major Grid organizations (EGI, XSEDE and NorduGrid).

The OSG security team reports significant incidents to the OSG executive team (ET) and the VO

representative (if the ATLAS VO is affected the U.S. ATLAS Facility Manager is informed). U.S.
ATLAS Management is immediately informed about the incident and reports to the funding agencies as appropriate.

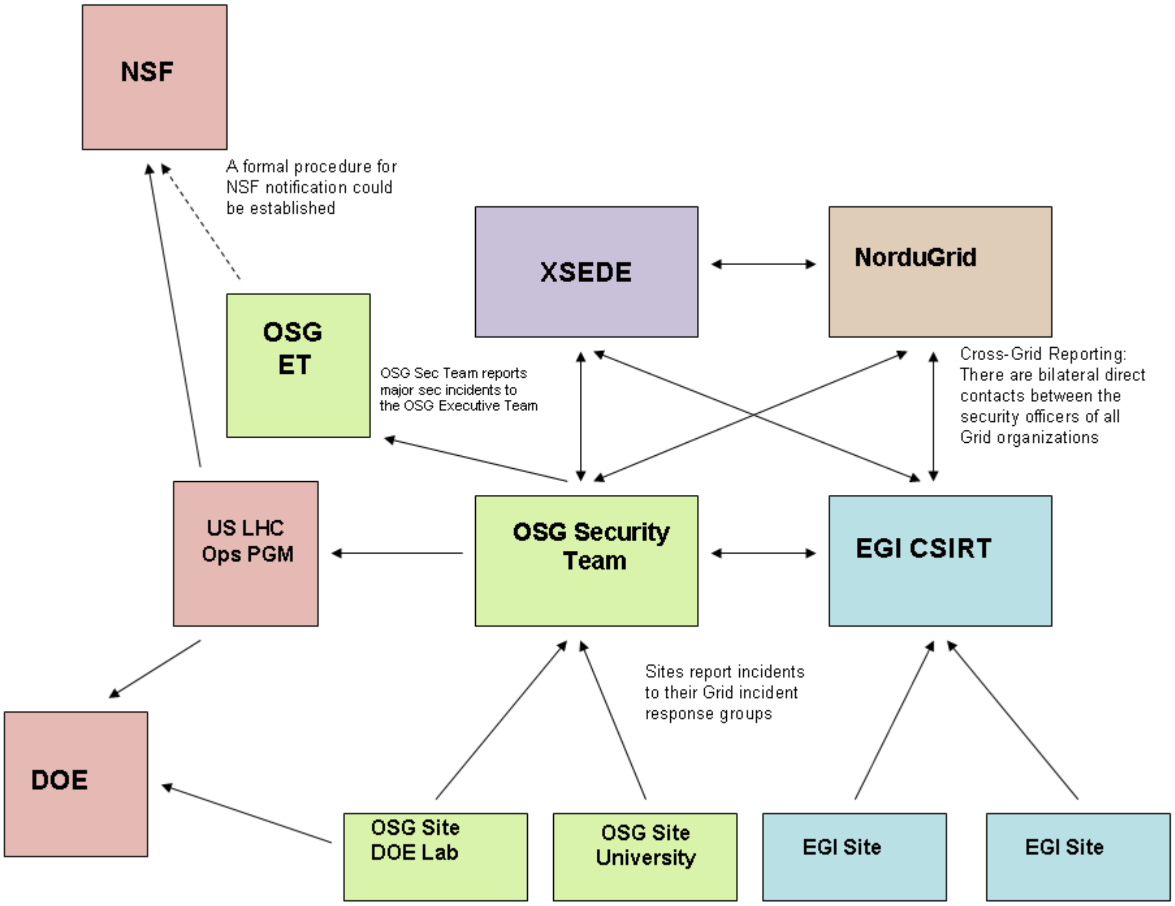
NSF
A formal procedure for NSF notification could be established
XSEDE
NorduGrid
OSG ET
OSG Sec Team reports major sec incidents to the OSG Executive Team
Cross-Grid Reporting: There are bilateral direct contacts between the security officers of all Grid organizations
US LHC Ops PGM
OSG Security Team
EGI CSIRT
Sites report incidents to their Grid incident response groups
DOE
OSG Site DOE Lab
OSG Site University
EGI Site
EGI Site

Figure 1: Cyber Security Incident Reporting Chain