**Survey-DATA**

*1) Which core service or asset are you reporting for?*

Three of them:

a) The Pacman caches, hosted at vdt.cs.wisc.edu

b) The VDT tickets system, hosted at crt.cs.wisc.edu

c) The software stack, which I assume is the Pacman caches + our subversion repository.

*2) Have you read the OSG Security Plan, Data Integrity section 2.3.3 within the past 12 months and understand your responsibilities for the proper handling of Sensitive Personal Data, Restricted Data, Limited Distribution Data and Public Data. This document can be found at the OSG DocDB website: https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=389*

No, not within the last 12 months.

*3) If your service does not store, process, transmit any data, you may indicate it here and conclude the survey.*

We store, process, and transmit data.

*4) Are you the owner of the data? The data owner is responsible for collection, storage, and treatment of the data. Although you own the core service/process, there may be another person who owns the data. If so, please provide his/her name below, and answer the following questions with that person.*

Yes, I Alain Roy, am the owner.

*5) Please enter data name you own along with a very brief description and the data type. The data types are explained in Section 2.4.3 https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=389.*

*5-A) Name*

*5-B) Description*

*5-C) Type*

You mean Section 2.3.3

Pacman caches. The packaging descriptions and tarballs for the OSG software stack. Public data

VDT tickets: The full text and file attachments for all VDT tickets. Public data except for security-related tikets.

OSG Software Stack: This is the Pacman caches plus our Subversion repository. Public data

*6) What is your data backup policy (e.g., weekly full, daily differential, etc.) ?*

Weekly. We rely on our local system administrators for backups.

*7-A) How long do you retain the back-ups?*

Unsure.

REPORT: It is recommended that they create a backup retention policy. This question is emailed to the CSLab.

*7-B) How do you ensure that your data back-ups are stored correctly, protected and restorable?*

We have done occasional but rare verification of this.

REPORT: For important data that needs to be backed up, we strongly recommend random tests for restoring from the back-ups.

*8) Please list your on-call support email address and/or phone number in case of emergencies, such as unexpected power loss, security attacks or natural disasters.*

vdt-support@opensciencegrid.org

*9) Are you aware of any attacks against the data? What do you think is the biggest threat against the data?*

I am not aware of any attacks. The biggest threat is the accidental loss or corruption.

REPORT: I would also add the risk of someone maliciously tampering with root-privileged executables.

*10) If you own Restricted Data please answer the following questions.*

No restricted data.

*11) If you do not own any limited data, skip to Question 12. If you have multiple data under restricted category and each one has dfferent answers for the following questions, please answer the questions for each data separately*

Our security tickets have restricted data.

REPORT: Security data is indeed limited type but this answer is also acceptable.

*11-A) Who is authorized to access the data? How do you determine this list of people?*

The VDT team

REPORT: Also the security team has access to the security tickets.

*11-B) How do you communicate the security requirements to the data to authorized recipients ? Do the recipients agree to the requirements? Do you keep record of such communications in a way that can be audited?*

We communicate informally and no records are kept of these communications.

*11-C) Which access control mechanims applies to this data?*

Username & password

REPORT: Is the uname/password sent over secure communication channels?Check whether someone without authorization can view the security tickets.

*11-D) Do you keep logs of access to the data? And if so, how long do you keep the log files?*

No, I don’t believe we have logs of access to the security tickets.

*11-F) What information is recorded in the log files?*

Everything in the ticket: all communication and attached files.

*11-G) How do you terminate rights of authorized recipients? Which mechanisms are used to achieve this?*

We remove their username and password by using the ticket system’s user management capabilitities.

*12) If you have any public data, please answer the following questions*

All of our data other than security tickets is public.

*12-A) What are the, if there are any, access control mechanisms applied to your Public data to maintain its integrity? (An example would be a list of the authorized people who can modify the data.)*

Unix username/password is used for local access, and a Subversion username/password is used for the source code repository.

REPORT: Is the uname/password sent over secure communication channels? Do you have a password policy on the strength of the passwords?

**ConfigMgmt**

1) Which core service or asset are you reporting for?

Three of them:

a) The Pacman caches, hosted at vdt.cs.wisc.edu

b) The VDT tickets system, hosted at crt.cs.wisc.edu

c) The software stack, which I assume is the Pacman caches + our subversion repository.

*2) Please indicate if you have read the OSG Security Plan, Configuration Management section 2.4.4 within the past 12 months and understand your responsibilities for Monitoring, Version Control and Security Review of the OSG Core resources under your control. This document can be found at the OSG DocDB website: https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=389 \**

No, not within the last 12 months.

*3) How do you ensure that your service's configuration variables are not modified by unauthorized parties? How can you detect if unauthorized changes are made?*

We rely on our system administrators. Only privileged users are allowed to make changes.

REPORT: This question has been sent to the CSLab

*4) Please indicate the version control system you employ for tracking changes to your service configuration. For e.g. do you maintain a change log that could be used to track and rollback any changes to configuration?*

We rely on our system administrators and don’t know how they handle this.

REPORT: This question has been sent to the CSLab

*5)Please indicate the process of approving configuration changes for your core OSG service. Specifically what steps are taken to review the security implication of the proposed changes*

We rely on our system administrators and don’t know how they handle this.

REPORT: This question has been sent to the CSLab

**VulnMgnt**

*1) Which core service or asset are you reporting for?*

Three of them:

a) The Pacman caches, hosted at vdt.cs.wisc.edu

b) The VDT tickets system, hosted at crt.cs.wisc.edu

c) The software stack, which I assume is the Pacman caches + our subversion repository.

*2) What system do you use to report and track vulnerabilities of your core service. E.g. Do you maintain vulnerability logs?*

We rely on our system administrators and don’t know what they use.

REPORT: This question has been sent to the CSLab

*3) What steps do you employ to mitigate vulnerability to your core services. For e.g. What types of vulnerability scanning are being done? Do you have regular scheduled updates/maintenance schedule to fix known vulnerabilities?*

We rely on our system administrators and don’t know what they do.

REPORT: This question has been sent to the CSLab

**Phys**

1) Which core service or asset are you reporting for?

Three of them:

a) The Pacman caches, hosted at vdt.cs.wisc.edu

b) The VDT tickets system, hosted at crt.cs.wisc.edu

c) The software stack, which I assume is the Pacman caches + our subversion repository.

*2) Please indicate if you have read the OSG Security Plan, Physical Access Control and Site Management section 2.4.6 within the past 12 months and understand your responsibilities for the OSG Core resources under your control. This document can be found at the OSG DocDB website: https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=389 \**

No, not in the last 12 months

*3) Physical access to all production core OSG systems must be controlled -- with a lock, key, etc.  Verify that your core OSG resources comply with this requirement and are indeed in an access controlled area, as defined above.*

Yes, they are restricted with locks. These are provided by our local building management.

*4) Who among your team currently has root and sudo access on the OSG systems providing core services and what is the policy of granting such access?*

The VDT team and our local system administrations. What does “sudo” have to do with physical access?

*5) According to the OSG Security Plan, network login or command line access to a production core OSG system shall be permitted only from a client via secure authorization and authentication mechanisms. Describe which authorization and authentication mechanisms you are using for secure network login or command line access by privileged staff versus unprivileged users.*

We use ssh.

REPORT: ssh with passwords? Recommendation is to use rsa keys.

*6) All production core OSG systems shall run the absolute minimum set of network services required for their functions. Have you verified in the past year that your core OSG resource systems are running only those network services necessary for system operation? Also list the network services running that are deemed NOT necessary.*

No, we rely on our system administrators. They do a good job, but I haven’t verified this.

REPORT: A verification of unnecessary services running on the server is strongly recommended.

*7) All production core OSG service providers must have a plan describing redundancy or other mechanisms used to maintain service availability in case of operational disruption or emergencies. Please describe the redundancy plans that would be deployed for your core service to ensure availability in case of unplanned disruption or emergency.*

We have no SLA for these services and therefore have not deployed redundant nodes. That said, all of our critical data is on a shared file system (AFS) with redundancy. Therefore it is not too hard to bring up new nodes with access to our data, if necessary. That said, we don’t have a redundancy plan in place.

REPORT: A data redundancy plan and exercise is recommended.

*8) On each production core OSG system, a copy of the system and service logs shall be saved on line for at least 30 days. Have you verified within the past year that this requirement is being met?*

No, I have not.

REPORT: It is recommended that service logs should be retained for 30 days and checked routinely for malicious access.

**Auth**

*1) Which core service or asset are you reporting for?*

Three of them:

a) The Pacman caches, hosted at vdt.cs.wisc.edu

b) The VDT tickets system, hosted at crt.cs.wisc.edu

c) The software stack, which I assume is the Pacman caches + our subversion repository.

*2) Indicate that you have read the OSG Security Plan, Access Control section 2.5.2 Scanning section 2.5.3 within the past 12 months and understand your corresponding responsibilities for the OSG Core resources under your control. This document can be found at the OSG DocDB website: https://osg-docdb.opensciencegrid.org:440/cgi-bin/ShowDocument?docid=389 \**

No, I have not.

*3) What authentication mechanism is employed for privileged access to core resources*

ssh, except for Subversion, which uses username and password.

REPORT: Is username/password sent over secure channels?

*4) How is privileged access to core resource granted and what authorization technique is used?*

Only local system administrators have access and the OSG Software Team.

5) What is the authentication and authorization techniques used for non-privileged user access?

ssh access is used for everyone, except for the publically viewable data from our web and subversion servers.

*6) At what frequency are you scanning web services for vulnerabilities and what types of vulnerability scanning are being done?*

I don't know—our system administrators handle this.

REPORT: This is sent to CSLab

*7) What remedial procedures are followed when vulnerabilities are detected?*

I don't know—our system administrators handle this.

REPORT: This is sent to CSLab

*8) What steps are being taken to scan for local vulnerabilities/intrusion detection and how often?*

I don't know—our system administrators handle this.

REPORT: This is sent to CSLab

Elaboration on the ssh access to VDT services. Captured during verbal communication with Alain Roy on 7/18/2011

All our services except the following uses ssh with RSA keys or Kerberos tickets.

vdt-itb.cs.wisc.edu: Our ITB computer for testing. ssh with uname/password, maybe RSA keys if people set up.

osg-edu.cs.wisc.edu: Our OSG-EDU VO computer for students. ssh with uname/password, maybe RSA keys if people set up.

vdt-bastion.cs.wisc.edu: Our computer that is used to hop to the private network. ssh with uname/password, maybe RSA keys if people set up.

\*test.cs.wisc.edu: Computers on private network for testing purposes. Can only use username password.

Further elaboration with David Parter of CSLab at u of Wisconsin.

Dear David, Thank you for your time answering my questions. Below is a summary of our meeting. Please let me know if I incorrectly stated something. --Level 0 full backups are done every two weeks. These backups are kept for a year. Incremental backups are done daily and retained between 30-60 days. There are no organized tests for restoring the data from the backups. CSlab staff usually gets a request once a month to do this. If there are no requests, then there are no restorations.

-- There are no attacks observed but they are not looking closely either

-- Configuration variables are only accessible to cslab staff. There is no formal process for changing the values. A staff member responsible for the area decides on the change. if there is a security concern they ask David.

-- Configuration mgmt system checks daily certain files and makes sure they are not incorrectly changed. The system overwrites the unaccepted values and sends an email to the lab staff. This is an home grown system similar to Puppet.

-- ssh access is used 99% of the time by the cslab members. They use kerberized ssh. They also allow root access via ssh. Kerberos is run by the cslab. David reviews the list of people in the cslab group twice a year. They have 7ftes and 10 undergrads.

-- There are no intrusion detection tools or application vulnerability scanners. They do not get any reports from the university security team.