Troy

The security review component of the Globus Online (GO) operation readiness review revealed a number of issues that require attention before the security group can recommend GO for deployment.

Specifically they are:

1. The backup of the Cassandra DataBase should address protection of private key materials. The ideal solution would not backup private keys. Acknowledgement that this has been addressed and documented will move this issue to - resolved.

   RESPONSE: Resolved. We have removed the private credentials from the Cassandra backups. This change was released to production on March 21, 2012. Older backups that include private credentials will be deleted (via our normal expiration policy on backups) within a couple weeks.

2. From the SD&I security discussion there were numerous concerns raised about inconsistencies regarding the lack of encryption of private keys in storage, while in transport, handled by backend services, and the general approach to management of private keys used to encrypt credentials. With respect to the mitigation there are three suggested strategies to resolve this issue, including:
   a. Implementation of limited proxies to reduce the impact of an executed vulnerability.

      RESPONSE: The Globus Online team agrees XSEDE should take measures to limit the impact of a compromised proxy certificates so that they cannot be used by an attacker to gain shell access, and that use of limited proxies is likely part of the solution. However:

      (1) We feel the recommended solution (having Globus Online convert all incoming proxies to limited) is inadequate, for two reasons:
      (a) Limited proxies, by themselves, are not sufficient to solve the problem. The intruder could still use the limited proxy to modify ~/.ssh/authorized_keys (or other ~/dot files) via GridFTP, and then login. To close this attack vector, XSEDE resource providers also need to configure their GridFTP servers to deny access to security related files and directories, which is a new feature in GridFTP version 5.0.5 and 5.2.1.
      (b) The XSEDE MyProxy must generate the limited proxy, rather than have Globus Online do this conversion. Otherwise, an attacker could still capture the full proxy when it is delegated to Globus Online, before Globus Online can create the limited proxy and throw the full proxy away.

      (2) We question why this is considered a show-stopper on acceptance of Globus Online by XSEDE. Proxy certificates are used extensively throughout XSEDE, and not just by Globus Online. This vulnerability has existed for a decade. Arguably Globus Online has reduced the risks associated with compromised proxies, by moving proxies out of the hands of a myriad of clients and into a professionally managed service.

      We argue that the right answer to mitigating this risk is to prioritize SD&I activities for deploying updated GridFTP servers with appropriate configuration, and extending the XSEDE OAuth MyProxy server to issue limited proxies to Globus Online. In the mean time, the risks associated with Globus Online's proxy cache do not seem sufficiently high to stall Globus Online's acceptance while we wait for these other activities.

b. Harden private key issues throughout via best practices (e.g., hardware security modules, not writing any plaintext keys to disk anywhere, implementing TLS/SSL on all backend communication channels, etc)

RESPONSE:

- "hardware security modules"
Our understanding is that a hardware security module to Globus Online would only add an additional hurdle, but it does not make the system more secure. If Globus Online is able to access a hardware security device remotely, then an intruder would be able to as well. What are the scenarios where a hardware security module would help prevent or reduce a security incident?

- "not writing any plaintext keys to disk anywhere"
Currently, we do store decryption keys and web server ssl keys on disk in plain text. If access is gained, then the intruder gains the ability to decrypt data stored in the Cassandra database, which includes the user proxies. We do this in order to allow automatic restarts of the Globus Online service. We view this as an acceptable risk for the benefit gained.

In the file transfer Postgres database we currently store the user proxies unencrypted. Given that access to database backups is limited to the set of developers that administer the system, we do not believe this is a likely attack vector. Even so, we will take steps to insure that no unencrypted private keys are present on backup medium. We estimate this will be added to Globus Online's production system by Q2 2012.

However, we need to have unencrypted proxies on (ephemeral) disk, as the client applications used by Globus Online to communicate with GridFTP servers receive credentials via files. Also, we do not see caching these credentials in memory as a significant security improvement. If Globus Online software running on the system can access an in-memory cache of credentials, then an intruder on the system will also be able to access these credentials.

- "implementing TLS/SSL on all backend communication channels"
We feel that TLS/SSL is not necessary for the internal Globus Online services that are only accessible from other processes within an Amazon security group. Communication between 2 two EC2 servers that are protected by security groups cannot be sniffed by processes that are external to the security group. Details:
http://aws.amazon.com/security/ "end-to-end privacy"
http://d36cz9buwru1tt.cloudfront.net/pdf/AWS_Security_Whitepaper.pdf "It is not possible for a virtual instance running in promiscuous mode to receive or "sniff" traffic that is intended for a different virtual instance."

We are happy to discuss these issues in more detail, and try to come up with improvements to the Globus Online service. But we do not believe these specific recommendations improve the security of Globus Online, and therefore should not be considered show-stoppers on acceptance of Globus Online by XSEDE. It would be helpful in subsequent discussions on this topic to describe the attack vectors that are of concern.

c. Implement more robust monitoring and audit capabilities. What is being suggested is to employ best practice monitoring. This mitigation strategy is at best a short-term solution and does not address longer-term risks and therefore should only be viewed as a short-term mitigation strategy. The recommendation includes:

i. Enable remote logging (Syslog) in addition to just storing logs locally. The latter makes logs susceptible to manipulation if a host is compromised.

RESPONSE: We have an effort well underway that will log all security related events including user authentication, administrator access, credential acquisition, and credential retrieval to a remote system via the syslog protocol. The logging collector will be secured such that logging clients will only have append access to the logs. Traffic between the clients and collectors will not be accessible by any third party other than the hosting provider. We expect to have this deployed and operational by mid-April.

ii. Implement file integrity checks to ensure that services and configuration changes are readily identified and appropriate steps are taken to validate changes.

RESPONSE: We have begun prototyping enhancements to Globus Online to use OSSEC to address this issue. We estimate this will be added to Globus Online's production system by Q2 2012.

Is this really a show-stopper for Globus Online acceptance by XSEDE? Can this be addressed in the next iteration of the Globus Online configuration item?

3. The Globus Online Security Review-Dec4-2011.pdf, which was done by Von Welch identified a number of recommendations, some of which have already been addressed, however we would like the Globus Online team to document their strategy and timeframe to address all of the concerns raised by Mr. Welch.

RESPONSE: Von Welch's doc is here: https://scholarworks.iu.edu/dspace/handle/2022/14147 Please see the GO-Von-Timeline spreadsheet of Von's items with description and timeline for when we expect to have a solution on production GO. In short, we expect to address all of these issues in Q2 and Q3 2012.

The security review team feels that the impact of an exploit from the identified GO vulnerabilities is collectively high, however we feel that the probability of an attacker leveraging them is low at this point. The threats associated with these vulnerabilities include both active malicious attacks against the identified vulnerabilities and accidental discovery of unprotected private keys and then active use of those keys. The overall risk level rating for these vulnerabilities is categorized as MEDIUM and need to be addressed before deployment is approved.

Randy Butler

XSEDE Security Officer