Security Q&A

Open Science Grid

OSG Site Administrators workshop
Indianapolis
August 6-7 2009

Doug Olson
dlolson@lbl.gov
LBNL

Account mapping concerns (1)

- *It seems the sites that map many GRID DNs to a single Unix account are opening up a security hole. Let's call the account griduser. Can't any GRID user running as griduser at that site gain access to the credentials for every other GRID user running as griduser at that site? In particular, can't grid proxies be stolen? If they are stolen what are the thieves able to do with them?*

- Primarily the risk is to the VO. If the VO is happy having all their users mapped to the same account then it is their data and resource usage at risk.
- Two different users mapped to the same account can steal each other's proxies. If it is a “limited” proxy them mostly it can only be used for gridftp. If it is an “full” proxy then it has the full privilege of the owner, for the remaining life of the proxy.

Account mapping concerns (2)

- *It seems there are some issues with mapping GRID DNs to real local accounts. If a grid proxy is stolen for the real account, then it is like the hacker now has elevated privileges. Perhaps access to ssh keys, ~/.globus, etc. I would like to see a discussion about how to setup the local accounts that will get mapped to DNs. How to keep a hard line between real users and grid users.*
- Very restrictive access rights
  - ❑ E.g. no shells
  - ❑ No interactive login
  - ❑ No coincidence with a real user’s account name
- (This is a good topic for the best practices guide).

Grid Proxies

- *Can't root at all GRID sites steal the grid proxies of any DN that runs on that site? Once they have the grid proxy are they able to then launch jobs on other sites where they might steal more grid proxies where they ... You get the idea. The big concern here is that every site on the grid relies on the security of every other site on the grid?*
- Yes, although normally a site only gets "limited" proxies so they can not be used to run jobs on other sites.
- The limited protections on proxies is a primary reason that they should have a short lifetime. It is a recognized defect in the grid software that a site can not put a limit on the lifetime of accepted proxies.

Rootkits: And other Files

- *What prevents a grid user from installing rootkits at my site? From attempting to download /etc/passwd, /etc/shadow, etc? Using the fork manager to perform reconnaissance on the CE? After all the CE is main way into the system. Allowing "strangers" to run on the main gateway into the system seems like asking for trouble.*

- The best protection against rootkits is rapid patching of vulnerabilities so hackers have less chance to exploit a vulnerability to gain root privilege.
- It would be good to have a different authorized user list for fork jobs than regular batch jobs. Can this be done?

Certificates

- *We have all had to click that button in the web browser where we make an exception for a CA. We have all done it so many times that we don't look at what we are doing anymore. Why doesn't the OSG use recognized CAs so that the third party is known and can be trusted? Aren't we opening up the system for "man in the middle" attacks?*

- There is some work towards having more IGTF CA's (including DOEGrids) to be trusted in web browsers.
- The CA package used to put CAs into the globus TRUSTED_CA directory is well controlled.
- A problem with existing commercial CAs is that their policies don't meet grid requirements (unique DN's).