Minutes
from the Security Session at
JRA1 All-hands meeting, Padova
Tuesday Nov. 16, 2004

Chair: Ake Edlund
Minutes: Gerben Venekamp.

VOMS
Joni Hakala, Valerio Venturi

See presentation. No comments from the audience.

Site access control issues (a sneak preview of DJRA3.2)
Martijn Steenbakkers

- Erwin: Language crossing, this imposes problems, because DAS uses Java, LCMAPS C. Perhaps this is a general issue? Martijn: Yes, but we can enter directly pass the VOMS attributes to LCMAPS instead of using the security context.
- Erwin: When get accounting integrated? Martijn: I hope before December 3
- Linda: CRL checking is integral part of authN, why is it also in authZ Martijn: requirement from siteaaa-group
- Linda: You need CRLs in order to do AuthN. Should discuss this in the JSPG.
- SO: (slide 6) what do you want to implement? Martijn: XACML
- Joni: CRLs are checked during TLS handshake, no need to redo it in authZ Martijn: requiremetn from SAAARG, will clarify/check. *Check: actually what was meant is that it maybe useful to do site-central CRL checking (the way the SAZ at Fermilab works), so the gatekeeper could delegate this to a central (authZ) service.*

The software formerly known as the Site Proxy
Oscar Koeroo

- Erwin: Agrees with proxy being too overloaded.
- Joni: It is possible to tie the policies to service types, like "allow access to storage elements"? A plugin that contacts the information system to get this information?

Slide 7

- Alberto: Firewall, is it a machine or is it software? What do you need to know about it? Oscar: This could be any of thinkable if it is a controllable entity
- Ferrari: What to does PortNumber/TCP correspond to? Oscar: this is referring to the connection a user wishes to setup
- Ferrari: Are performance penalties from firewalls considered? Oscar: performance hits are only there when you open a port. Not in transfer. That is limited to the firewall or router infrastructure that is in place.

- Ferrari: Have you (JRA3) considered MPLS as an alternative to firewalls? Oscar: No we will take a look at it
- Francesco P: How do you protect the service? Only let authorized users connect. Oscar: Use router to limit the allowable IP numbers for connection. Joni: WS will connect to the real service, thus providing necessary protection.
- Francesco P: How do you sell your solution to the local sysadmin? Oscar: there are setups thinkable to test this and get comfortable with this system
- Francesco P: How do you propagate policies from one site to another? Oscar: No, just as we don't with other policies
- Francesco P: How to prevent an executable from using local exploits to become root? How to convince the local sysadmin of security?
- Francesco P: Is there a foreseen way to ask the service for a private policy? Oscar: We will use XACML, Andrew is working on it. So we could publish if feasible

Coffee break

Security in DM
Akos Frohner

- Erwin: If a proxy has **expired** is it renewably? Joni: the service will refuse it. SO: If you have a proxy you can renew it, if you have not, you cannot. Akos: wants a proxy for file transfers to establish a trust relation. This may be a limited proxy. Joni: is there an implementation for the trust relation. Akos: No. Joni: If you implement that in MyProxy you are doing Message Level Security. Akos: I like to use the components that are available now.
- Erwin: How does negotiation port type by JRA3…? Akos: First phase we have to do delegation; how to use us is not important. We could use delegation port type or GSI. Erwin: Does it work now. Akos: yes, we have something working.
- SO: Can the service be replaced by GAS: Akos: yes, the backend can be replaced.
- Linda: Would it be possible for the user to sign a request for data ticket…? Akos: …Message level security implementations are not ready yet.
- Ake: What are you feelings about level message security? Akos: It is a matter of trust. We do not have a perfect system yet.
- Erwin: *(last slide)* How many of these issues are showstoppers? Akos: It would [will] work.

List of issues
Joni Hahkala

- SO: *(slide 4)* Third solution comes closest to what I think.
- Akos: There seems to be some confusion. If you use DN or grid username, we will return that string.
- Akos: there are six solutions. These have been discussed before. Do we want to re-discuss them again with their pros and cons?
- Joni: assert that VO names are unique.
- SO: who is the registration authority? Akos: Kerberos database.

- Joni/Ake: simplest solution is something we have to do anyway.
- SO: VO is a CA because it is issuing its own certs.
- Linda: objections to third solutions. Have a tool that manages people's grid identity.
- SO: If I change my "identity" and my cert expires, what then? SO: The point of cert is precisely like that. Erwin: What if I stay in the same VO? SO: fix your cert, not the other way around. Joni: You are still the owner of the files (of your old cert). You would like to access them with your new cert. [if you are still within the same VO]. SO: Do you still need access to your files five year after expiration of your cert.? Joni: there is still a lot to discuss about this topic.
- Joni: Go for the first solution. Does not solve all problems, but is good enough for now. You can have multiple VOs.
- Joni: Agreed to disagree about final solution [SA1?]
- Ake: we will do the first solution, because we will need it anyway. And will explain what it solves and not.

C/C++

- Never said that **C**/C++ communications not solved by Grid. We considered the Apache server, but it was too heavy and didn't provide the level of control we require. Decided not to go that way. We implemented minimal http server to cover our requirements. Currently we have no reason to abandon this approach. Can talk to any client which used SSL implementation.
- We write our won plug-in.
- LD service uses its own… GSOAP for services.
- Akos: Data management point of view, is it separated from other services?
- We in favour of converging to one solution.
- Joni: come and visit CERN. Yes, we can have a discussion.

GPBOX:

- GPOX is a policy frame work from JRA1. Presentation at CHEP [2004]. Policy management tool for managing policies. It is based on XACML. Does is help with security: Martijn: Yuri works on XACML within JRA3. Andrew as well. Martijn to write an email to connect Vincenzo, Yuri and Andrew.