General Questions Not Relating To A Specific Paper:

Lee Smith: Somewhat unrelated to the subject matter of the paper, why does the military have the policy of "read down and write up"? Why wouldn't it be "read down and write down"?

Corban Rivera: many of the systems we have looked at use LDAP repositories for storage. What is the advantage of LDAP over other methods of secure storage like DBMS?

The PRIMA Grid Authorization System

Fine Grained vs. Course Grained

Ranjit Randhawa: Could you explain the differences between fine-grain and coarse-grain privileges? Does this just apply to the action taken as a result of a particular privilege? What levels/types of privileges can users (who are able to delegate privileges), assign to others?

Glen Fink: I don't understand grid computing enough to see why the authors claim PRIMA is fine-grained. Doesn't the OS already provide privileges to this granularity? Is it because GLOBUS without PRIMA is coarse-grained? Is one of PRIMA's contributions that it extends recognition of OS into the grid computing world?

Muhammad Abu-Saqr: How does fine-grained access right differ from coarse grain privilege?

Scalability & Performance

Varun Pandey: The PRIMA paper talks of delegation. Is there any specific limit to the delegation level? How would the delegation be revoked if the level of delegation goes very deep? I mean is it by the certificate chaining as in SPKI or how else?

Varun Pandey: In section 3.5.2 the PRIMA paper talks of Grid Access Control Lists. I feel the list can become fairly large if the number of users increase? This is a common problem with the ACLs. I feel role based access would have been better. The only justification given is easy authentication using DNs. But what about the management of every entity which has ACLs? Like if the Organization of a user changes won't it create a problem to track each entity, check its GACL and change it if the particular user's DN is in the GACL.

Dynamic versus Static

Glen Fink: How do PRIMA's dynamically created policies differ from the underlying static access control policies? Are they like dynamic firewall rules that create a short-circuit in the authorization process for already-approved accesses?

Glen Fink: Are the "obligations" sent from the PDP to the PEP the embodiment of PRIMA's dynamic policies? Does this change the PEP into a sub-PDP?

Glen Fink: What are "dynamic accounts"? Are these accounts managed solely by PRIMA/GLOBUS, or do they correspond to some user account in the underlying OS?

Muhammad Abu-Saqr: What is the overhead used to identify party as authoritative party? If PDP already query these parties and then have a list could classified ad authoritative parties. What happen if one authoritative party compromised just after the last query?
Mechanism, Limitations, and Implication of Choices in Design

Corban Rivera: What are mechanisms to convey resource policies in grid environments?

Glen Fink: Providing reasons for denied access is good in general, but could that policy help a malicious user learn more quickly how to obtain the access he wants?

Glen Fink: What advantages motivate the use of proxy certificates in PRIMA as opposed to simply using identity certificates?

Glen Fink: If PRIMA authorizes permission to a file based on the POSIX permissions at the time the access is requested, what happens if the file owner restricts access to the file subsequently? Does PRIMA honor changes to the underlying access flags dynamically?

Darrell Hyatt: (pg. 6) Allowing the user to select which privileges should be applied (as a way of enforcing least privilege) puts a lot of trust in the grid user. While I would presume that a grid user is more skilled than a run-of-the-mill user, is this a good idea?

Darrell Hyatt: (pg. 6) Does the user actually choose which privileges to apply or are they "chosen" for him by the system when he makes his request?

Darrell Hyatt: (pg. 9) Was there a reason that the Pull model was preferred to either of the other two?

Darrell Hyatt: Assume that I am creating a delegate privilege based upon some subset of my own privileges (an industry partner needs access for only the next two weeks). Can I accidentally (or intentionally) give my delegate a lifetime past my own (my privileges expire at the end of this week)? (I would assume that I would have to renew my own privileges first)

Muhammad Abu-Saqer: In grid computing the number of resources is not stable since new resources enter the grid as other leave, how PRIMA is a good security solution with this rapidly change environment with its property that it should the PDP should queries each party.

Security

Muhammad Abu-Saqer: In most occasions, the network administrators disable the guest account since it could use by some attacker in bad way. When a grid user granted a user account, which in this case it could has more privileges than the guest account could this account use to compromise the hosting system or used to launch attacks to other grid resources or systems.

Execution Environment & Operating System

Muhammad Abu-Saqer: In practice what is the execution environment?

Muhammad Abu-Saqer: Does PRIMA require changes or extensions to the core of the operating system?

Muhammad Abu-Saqer: Could PRIMA work under windows?

General

Varun Pandey: I didn't quite understand figure 3-3 in the PRIMA paper. Specifically, how is the HOLDER in the last Attribute Certificate become the ISSUER in the last Proxy certificate?
Glen Fink: The discussion of the difference between the full association of PRIMA's privileges vs. the implicit association offered by capabilities or ACLs is unclear to me. Could we examine this more closely?

Darrell Hyatt: Can I define a delegate privilege based upon an access right that I have through a group membership?

Muhammad Abu-Saqer: how PRIMA could apply to the new resources that just joined the grid.

**PERMIS X.509 Role Based Privilege Management Infrastructure**

**Revocation & Consistency**

Darrell Hyatt: It seems that any problems related to propagating revocation or privilege change would be worse in the authorization realm than they were in the authentication realm.

Aparna Sharma: Each XML policy has been given a globally unique object identifier by SOA during its creation. What happens when policies are removed or updated or merged with other policies? Can there be a potential case where reference to a policy which has already been removed is made?

Ranjit Randhawa: What happens to the certificate and/or attributes when certified attributes, which are stored directly in the certificate, are changed? Can it work with other authentication systems, like Shibboleth?

Glen Fink: Are role ACs cached locally, and does this lead to potential inconsistency with the AC database stored in the LDAP?

Muhammad Abu-Saqer: If the certificate revoked does this imply the attribute is revoked as well?

**Application Specific or Independence**

Aparna Sharma: The paper states that authentication is performed in an application-specific manner but authorization is performed in application-independent manner. Could any of the application specific details be required for authorization or in all the systems authorization is independent of the underlying application?

**PMI vs. PKI**

Lee Smith: In the X.509 PMI the access rights are held within the privilege attributes of ACs issued to users. Is there this really a secure way of dealing with authorization? I know they are trying to draw a parallel between PMIs and PKIs, but authorization and authentication are inherently different. Would it be feasible to forge an attribute certificate? Are there any other barriers that would prevent a forged certificate from being used?

**Scalability & Performance**

Varun Pandey: As i see the mapping of certificates in PERMIS, its as follows:

- name -> key (issued by a CA)
- name -> roles (issued by a PA)
- roles -> permissions (issued by a PA)s

So in (a) and (b) steps the CA and the PA must agree to a common namespace. Can this create
some problems some time? Maybe if one thinks at an international scale.

Aparna Sharma: PERMIS can operate with any authentication policy (Shibboleth, Kerberos, PKI). Can PERMIS leverage on any of these authentication policies and perform better? Also is a combination of any these authentication policy more secure with PREMIS than the other?

Aparna Sharma: At each attempt to perform actions on the target, the AEF passes the target name and the attempted action along with its parameters, to the ADF via a call to the Decision. The user may attempt arbitrary number of actions on different targets and Decision is called for each one. This passing of parameters for each attempt is costly in terms of bandwidth. Should the Decisions be made just based on the target once and not based on number of attempts by the user on the same target?

Aparna Sharma: PERMIS assumes that the Target and the AEF are either co-located or can communicate with each other across a trusted LAN. This simplification of the AZN API is not always possible in all real world scenarios. This should certainly be an issue for deploying PREMIS and would limit its usage.

Questions of Motivation & Classification

Aparna Sharma: PERMIS can work in either push or pull mode. When is one mode preferred over the other?

Varun Pandey: The authors talk of delegation in RBAC usage in PERMIS. So isn't this then DAC?

Darrell Hyatt: What is the benefit of having authorization certificates? I don't need authority to use a service unless and until I actually intend to use it, so why bother with a certificate at all?

General Questions

Aparna Sharma: Does PERMIS support Policy inheritance? i.e., inheritance of subordinate policies from the root policy.

Muhammad Abu-Saqer: Why X.509 need to LDAP directory?