

Chris Willing  
University of Queensland, Australia

for:  
Future Security Issues for the Access Grid  
A User Perspective  
11<sup>th</sup> June, 2004

When I was asked to prepare a 15 minute presentation of the user's perspective for this panel session, I was somewhat confused as to what I could contribute. After all, I've never been very interested in security issues – a necessary evil maybe. So, what could I add to such a panel?

I eventually decided that since I'm supposed to be representing the user's perspective, my ignorance of security issues is probably quite appropriate (and makes for a very brief presentation!).

My experience as an Access Grid user goes back to 2001 when we built our first node (at the University of Sydney) for participation in that year's SCGlobal conference.

(That task was put to me by Professor Bernard Pailthorpe, who is the founding father of the Access Grid in Australia. While at SDSC he recognized the potential of the AG and when he returned, building a node was one of his first priorities.)

From that beginning of a single node for SCGlobal 2001, Australia now has about a dozen registered nodes with another half dozen under construction. These nodes are mostly within Universities, with just a few outside the education system. It is here that the first "user perspective" related security issue becomes apparent; that of expectation. Different users have different security expectations. These expectations may often actually be an institution's expectations, which the user working for that institution is required to adopt.

In an educational setting, we are generally trying to make the AG easy to use and accessible. Any security protection, e.g. firewall to navigate, is an unwanted hoop to jump through. On the other hand, commercial organizations seem to feel better, the more they spend on the security industry's latest offering. Unfortunately, this is becoming a trend in universities too.

Back at the University of Sydney, my old department has recently installed a desktop AG node in the office of a faculty Dean. In this context it is understandable that various communications (budgets, personnel issues) would require a high level of security, yet we wouldn't expect a high level of technical expertise from the user. This illustrates a second "user perspective" issue to consider; that of a user's capabilities. Whereas most attendees here today would be fairly tech-savvy, this will be less likely in the future; as ease of use of the AG tools increases, adoption by "inexperienced" users will

increase too. More and more nodes will be operated by users who have only limited technical capabilities.

Having looked briefly at two aspects of users themselves, namely user's expectations and user's capabilities, lets now consider three technological levels at which these two user groupings may face security issues.

1. Infrastructure: institutional/departmental policies e.g. firewall rules, are generally regarded a plague by both the user cases, although grudgingly accepted as necessary, especially for some particularly accident-prone operating systems.
2. Application/Session: the AG toolkit's use of Globus tools and public key infrastructure (PKI) generally is well regarded, satisfying corporate users. On the downside, the authentication transactions themselves appear to delay the entry to or change of rooms.
3. Media: the ability to encrypt media streams is highly regarded. However a room with encrypted streams is not in itself sufficient to ensure a private meeting; anyone with a valid proxy may enter the room, unless an access control list (ACL) has been configured for it. There is no mechanism for ordinary users to set these ACLs in the venue servers currently used for most meetings (at ANL, NCSA, APAG). The problem is typified by the following email extract:

*I think the first and foremost thing is ... how can someone set up secure meetings – easily. Currently there seems to be no (obvious) way of (from within AG2) (a) setting a key for vic/rat streams, (b) distributing that key securely to the relevant parties and (c) making sure that only people with particular certificates are able to access those keys. Maybe this is already in AG2.*

The author of this email extract is technically quite competent, yet is unaware of how to initiate a secure meeting; what about the less technically competent then?

In another recent email, I was asked to raise the possible use of the SRTP (rfc-3711) to secure RTP sessions. Perhaps this could be discussed in the discussion time?

More generally, whatever media encryption scheme is used, its impact on latency should be kept in mind. While vic's current encryption scheme seems OK (minimal latency increase) for the H.261 streams we currently use, this is not guaranteed for bigger media payloads. For instance, how would it impact on the HDTV streams demonstrated earlier at this retreat?

In summary, I've suggested that there are two user oriented continuums which should be considered as important factors in Access Grid security:

1. user expectations
2. user capabilities

I've also suggested that each of these user continuums is affected at three distinct levels of technology:

1. Infrastructure level
2. Application/Session level
3. Media level