Authentication: Implementation Issues and Strategies  
Birds-of-a-feather Session  
CAMP Boulder, CO June 3-6, 2003

It is conceptually important to think of the architecture as a network identity system composed of the credential, netid services in support of the credential, and netid-enabled applications that make use of the netid services and the netid. Anything can sit in the middle; multiple registries, or more exotic designs, but when it comes to controlling access to the resources within the identity management system, leverage what's already been built.

Three methods of authentication these days, and they should all be enterprise-class authentication systems: LDAP, Kerberos, and PKI. A near-term goal is to support some form of credential conversion between these. It's very difficult for people coming to this environment to understand the implications of each approach to enterprise authentication. No matrix exists of the advantages and drawbacks of the choices.

Often requests come in which are technologically difficult, or shouldn't be answered, such as, "Can you give me a list of all students and staff?" Many people in the campus environment will say, "Just give me the data and I'll deal with it." It is the job of the enterprise directory to store and provision this data, however, and administrators must carefully guard that. A useful way to do this is to make it clear that the enterprise directory doesn't "own" the data, although it is the authoritative source; it belongs to the registrar, and if the registrar gives permission, then they get to access the data.

Passwords are very difficult to have in one place. In Princeton, there are over 31 different password repositories; their goal is to reduce that to five or three: LDAP, Kerberos, and AD, and keep the passwords synchronized between them. There are applications that utilize LDAP, those that use Windows authentication, and those that employ service tickets; because so many applications rely on so many types of authentication, it is difficult to reduce the primary password store any further. Pushes to make sure all passwords go over secure channels can mean migration away from older protocols such as POP.

One of the primary considerations in selecting an authentication architecture is the vendor products that must be supported by it. The question sometimes isn't what to build, but how to connect to these products. In Michael's experience, it's important to get out from being on the back-end where a product simply arrives to be used as delivered, and to instead communicate with vendors in the contractual interactions to ensure that there's technological compatibility as well.