AAA & Security Breakout

Future CI Meeting, October 2, 2014
Marshall Brinn (BBN)
Julio Ibarra (FIU)
Vinod Mishra (ARL)
Stephen Nightingale (NIST)
Robert Ricci (Utah)
Vas Vasiliadis (UChicago)
Primary Discussion

- Globus identity services
- GENI identity and authorization framework
- Campus needs
- DoD needs
- Alternative key and attribute dissemination
- What’s needed for accountability (third ‘A’)
Authentication

• Where to draw trust boundaries
  • Are tools trusted?
  • How are assertions conveyed?
• Speaks-for in GENI
• Linking identities in Globus
Authorization Styles

- Gloubs: group-based, local filesystem ACLs
- GENI: Mix of groups, capabilities, attributes
- Time-limited
- Users from different source get different resources
- Limits on visibility of group membership
Uses of Accountability Data

- Holding someone responsible for bad behavior
- Identifying those using excess resources
- Improving operations
- Hard to draw the line between accountability and "just" logging
DNS-Based Trust Infrastructures

- Distributed database w/ caching
- Secured with DNSSEC
  - Single-rooted
- Easy to query
- Short caching time -> simple revocation
Campus Needs

• Making things simple for users

• Connection with Science DMZ

• Connect with variety of products, including commercial

• Question: User is the researcher or the service?
Needs for Sensitive Resources

- Strong partitioning between trust domains
- Isolation for classified data
- HIPAA compliance is not an on/off switch
- Multi-jurisdiction
Next Steps

• Need better tools for analysis for accounting
  • Consider public release of data
• Prototype signing GENI up as an IdP with Globus
• Try storing ssh keys or attributes in the DNS
• Look at technologies for separation of sensitive data