GRID SECURITY
for Grid Computing

Steve Sones
Grid Security
Grid Security - Outline

• Brief introduction to grids
• Grid security basics
• How grid security really works
• Good and bad facts about grid security
• Proposal
• Conclusions
• References
Grid Security – Background

How It Works

1. Main cluster server divides tasks into subtasks and parcels subtasks to local cluster servers.
2. Local cluster servers find available processing power on local PCs and distribute subtasks to those PCs.
3. Local cluster servers gather completed tasks from local PCs and send data back to main cluster server.
4. Main cluster server aggregates completed tasks and sends data to database farm.

In the global grid computing scenario, unused processing power on local clusters of computers scattered across the Internet would be harnessed to address a single, complex application.
Grid Security - Basics

- Delegation
- Security
- Community Authorization
**Grid Security - How does it really work?**

1. **User**
   - a. User gets Grid account
   - b. User invokes service to get grid certificate
   - c. Send password
   - d. Return user cert, user key

2. **Certificate Public Key**

3. **Certificate Authority**

4. **GRID Machine**

---

**Diagram:**
- User initiates a request for a grid certificate.
- The user is authenticated by the Certificate Authority (CA).
- The CA sends the public key to the user.
- The user uses the public key to request a certificate from the GRID Machine.
- The GRID Machine returns the user certificate and private key to the user.

---

**New Mexico Tech**
Grid Security - How does it really work?

1. Certificate Authority
   - Certificate
   - Public Key
   - Proxy Certificate

2. Portal
   - Invoke service to obtain Globus proxy

2.1. My Proxy Server
   - Return proxy file
   - Generate limited proxy file

2.2. Proxy server
   - CA

User
   - Invoke service to obtain Globus proxy
   - Return proxy file
Grid Security - How does it really work?

1. User invokes service to obtain Globus proxy.
2. SSH sends user cert, user key, pass-phrase, and time.
3. Proxy server generates time, limited proxy file.
5. CA certificate public key.

New Mexico Tech
Grid Security - How does it really work?

Proxy Certificate

Service

Client

New Mexico Tech
Grid Security - How does it really work?
Grid Security - How does it really work?

1. Certificate Authority
2. Proxy Certificate
3. Service Client
4. Request Params

Certificate Public Key
Proxy Certificate
Portal
My Proxy Server
SOAP Server
Web Service

New Mexico Tech
Grid Security - Pluses

- Employs a single-sign-on, run-anywhere authentication service
- Uses Public Key Infrastructure (extensions of X.509)
- Time limited proxy certificate
Grid Security - Problems

• Grid Security Infrastructure (GSI) security
  Using X.509 certificates has various limitations. For example:
  – If a user does not use a pass phrase, anyone that puts a hand on the certificate can use it.

• Others
  – Weak accounting (due to distributed control system)
  – ‘The firewall problem’: In order to submit a Globus job, some Internet ports must be opened.
Grid Security - Proposal

- Research (and implement) three middleware toolkits
  - Alchemi
  - Condor-G
  - Globus
- Study security vulnerabilities of each toolkit
Grid Security - Conclusions

• Security aspects in grid computing have such an important role due to the diverse and/or scattered resources and services.

• Continuing research in grid security is a challenge for a more secure grid computing environment.
Grid Security - References


Ashraf Memon. GSI Authentication on Web Services.  

http://web.syr.edu/~jraphael/Grid%20Computing.ppt