Global Grid Forum
GSS-API Extensions

Douglas E. Engert

DEEngert@anl.gov

Argonne National Laboratory

08/02/04

Introduction

- The Global Grid Forum
- The Globus GSI
- GSS-API Extensions

Global Grid Forum

- http://www.ggf.org
- Standardization of Grid Computing
- 400 Organization in 50 countries
- Next meeting; Sept 20-23, Brussels, Belgium

Characteristics of Grid Computing

- More then client server or distributed computing
- User-to-user, peer-to-peer authentication
- Users may start servers
- Delegation in both directions

The Globus GSI

- http://www.globus.org
- A GSS-API implementation using TLS/SSL with X.509 certificates
- Delegation using RFC- 3820 “Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile”
- Initiator and accepter use similar credentials.
- Allows “user-to-user” and “self-to-self”

GSS-API Extensions GFD-E.024

- http://www.ggf.org/documents/GWD-I-E/GFD-E.024.pdf
- http://www.ietf.org/internet-drafts/draft-engert-ggf-gss-extensions-01.txt (older)
- Describes extensions to the GSS-API made by the Globus Project to address deficiencies
- Describes additional functionality

Extensions

- Credential export and import
- Delegation at any time in either direction
- Credential extensions handling
- Setting of context options

Credential export and import

- gss_export_cred(), gss_import_cred()
  - credentials to a buffer. Application saves and reloads.
  - credentials saved for use by non GSS-API applications.
- Applications must be able to accept multiple connections, and save and reload the delegated credentials. Not tied to process or thread.
- Application can save and restore even over a reboot. For example batch job scheduler.
- Implemented for GSI and MIT Kerberos

ARGONNE NATIONAL LABORATORY • UNIVERSITY OF CHICAGO •

Concerns with "cred store"

- draft-williams-gssapi-store-deleg-creds-01.txt
- Needs more control by application over delegated creds
  - » Uses the implicit cred store, but does not address explicit cred stores under application control
- Refers to GGF GSI Extensions implying that the mech needs knowledge of environment
- Used Simon's OpenSSH mods as example. Yet Simon's mods passes back a KRB5CCNAME to be set in environment
- http://grid.ncsa.uiuc.edu/ssh/
- http://grid.ncsa.uiuc.edu/gssapi-mechglue/openssh/

Delegation at any time

- gss_init_delegation(), gss_accept_delegation()
- Allow delegation after context established.
  - Uses same call loops as init and accept.
  - Allows application to review connection and set options
  - Can be used to refresh credentials.
- Delegated credential may be different then that used for connection.
  - May even be credentials from different mechanism too!
- Delegation in either direction.

Credential extensions handling

- gss_inquire_sec_context_by_oid(), gss_inquire_cred_by_oid()
- Get mechanism or OID specific information from credentials. Possible uses:
  - Certificate extensions
  - Kerberos authorization data
- Use OID to avoid non mechanism API calls.
- Buffer set functions to handle the data

Setting of context options

- gss_set_context_option_call()
- Sets options for context using an OID. For example:
  - Limited delegation, restrictions
  - Kerberos forwardable flag
  - What to do when context expires
  - Set encryption options
- May be called before gss_init_sec_context and gss_accept_sec_context
  - Creates the starting context on first call

Additional functionality

- Token Framing for every token
- Levels of verbosity with gss_display_status
- Need a simple authz function, to access krb5_kuserok or the gridmap file

The End