GridSite security update

Andrew McNab

University of Manchester

Outline

- Credential types
- Attribute URIs
- New chain checking
- API clarifications
- Logging
- Level of Assurance
- Shibboleth

GridSite

- GridSite consists of
  - A grid security toolkit for C/C++
    - Parses GACL policies, X.509, GSI, VOMS credentials
  - An Apache module which adds support for these credentials
    - This lets people host webservices for Grids, written in C/C++/scripts/Java etc etc.

Credential types

- Four credential types supported up to GridSite 1.4.x
  - X.509 Distinguished Name
  - VOMS Fully Qualified Attribute Name
  - DN List groups
  - Client DNS hostname
- Stored in GRSTgaclCred structs in memory
- And as different <”credential”> containers in GACL 0.1 access policies.

In GACL 0.1

```
<gacl version=”0.1.0”>
<entry>...credential(s)...
          <allow><read/></allow></entry>
</gacl>
```

```
<person><dn>/DC=com/DC=example/CN=joe</dn></person>

<voms><fqan>/VO/group</fqan></voms>

<dn-list><url>https://example.com/group</url></dn-list>

<dns><hostname>example.com</hostname></dns>
```

Additional credentials

- Several new credential types “in the air”
- Have added Shibboleth support to GridSite, which introduces LDAP derived DNs.
- OpenID has http: URL-based IDs (and now xri:)
- Applications may need more
  - Verified email address
  - Kerberos/AFS user@domain
- All of these look like URIs ...

Attribute URIs

- Represent all credentials in URI “scheme:path” form
  - dn:/DC=com/DC=example/CN=joe
  - fqan:/VO/group
  - https://example.com/group
  - dns:example.com
  - ip:127.0.0.1
  - mailto:joe@example.com
  - kerberos:joe@example.com
  - https://example.com/openid/joe

In GACL 0.1

```
<gacl version=”0.1.0”>
<entry>...credential(s)...
        <allow><read/></allow></entry>
</gacl>
```

```
<person><dn>/DC=com/DC=example/CN=joe</dn></person>

     <voms><fqan>/VO/group</fqan></voms>

  <dn-list><url>https://example.com/group</url></dn-list>

   <dns><hostname>example.com</hostname></dns>
```

In GACL 1.0

```
<gacl version=”1.0.0”>
<entry><cred><auri>scheme:path</auri></cred>
        <allow><read/></allow></entry>
</gacl>
```

<cred> can also optionally include

<loa>level</loa> for Level of Assurance

and

<delegation>level</delegation> for GSI Proxy Delegation

“Bag of attributes”

- GridSite 1.5.1 onwards handle users as a set of semi-opaque attributes which policy engine checks for
  - Currently, some credentials are like this (eg X.509 DNs)
  - But others (eg DN Lists) are checked by the policy engine itself, finding the list of DNs that defines that group
- Now all attributes are loaded at the start
  - This means that “downstream” users of GridSite will get a list of DN Lists for that user too
  - So VOMS DN Lists can now be pre-fetched by sites, which are indistinguishable from FQANs from attribute certificates.
  - This allows attribute pull, which is esp. convenient for websites

GRSTx509ChainLoadCheck

- New function for checking and loading X.509 certificate chain
  - Takes STACK_OF(X509) as input
  - GSI-aware checking of chain back to CA root certs
  - Verifies VOMS attributes if present
  - Puts all of these into GRSTx509Chain struct
- This function is now (1.5.x) used by mod_gridsite within Apache, and by command line clients (htproxyinfo)
  - This avoids some duplication of code, and means only a single pass through the chain within Apache to verify and extract credentials

htproxyinfo output

```
localhost.mcnab: ./htproxyinfo
0 (CA) /C=UK/O=eScienceCA/OU=Authority/CN=CA
 Status     : 0 ( OK )
 Start      : Fri Jul 14 17:32:55 2006
 Finish     : Fri Jul 15 17:32:55 2011
 Delegation : 0
 Serial     : 1
 Issuer     : /C=UK/O=eScienceRoot/OU=Authority/L=Root/CN=CA

1 (EEC) /C=UK/O=eScience/OU=Manchester/L=HEP/CN=andrew mcnab
 Status     : 0 ( OK )
 Start      : Mon Oct 23 16:29:05 2006
 Finish     : Thu Nov 22 15:29:05 2007
 Delegation : 1
 Serial     : 8700
 Issuer     : /C=UK/O=eScienceCA/OU=Authority/CN=CA

2 (PC) /C=UK/O=eScience/OU=Manchester/L=HEP/CN=andrew mcnab/CN=proxy
 Status     : 0 ( OK )
 Start      : Tue Jun 12 10:10:38 2007
 Finish     : Tue Jun 12 22:15:38 2007
 Delegation : 0
 Serial     : 8700
 Issuer     : /C=UK/O=eScience/OU=Manchester/L=HEP/CN=andrew mcnab

3 (AC) /dteam/Role=NULL/Capability=NULL
 Status     : 0 ( OK )
 Start      : Tue Jun 12 10:15:38 2007
 Finish     : Tue Jun 12 22:15:38 2007
 Delegation : 0
 User DN    : /C=UK/O=eScience/OU=Manchester/L=HEP/CN=andrew mcnab
 VOMS DN    : /DC=ch/DC=cern/OU=computers/CN=voms.cern.ch
```

API clarifications

- Rationalising and properly documenting C API
  - Aim to have a clean API by 2.0
- Already quite modular
  - GRSThttpXXX(), GRSTx509XXX(), GRSTgaclXXX(), ...
  - Object-orientated with objects as structs and NounVerb access functions
- But currently lacking proper documentation on how to use all this in applications / services
- C++ / Perl / Python wrappers still on the roadmap

Logging

- GridSite library functions have to work inside command-line tools, CGI programs, Apache modules and standalone servers
  - Four quite different logging environments: stderr, /dev/null, ErrorLog, and syslog
- Now provide GRSTerrorLogFunc modelled on Apache ap_log_error() and syslog()
  - Can be overridden to use Apache, Syslog or stderr
- Apache error and access logs can themselves be sent to syslog, potentially including client DN etc.

Level of Assurance

- As part of FAME project we added “NIST-inspired” LoA conditions to GridSite/GACL
  - Can put requirement on a particular credential's LoA
- This information can either come from FAME extensions to Shibboleth
- Or be inserted by mod_gridsite itself
  - Map level 2 to GSI proxies
  - Map level 3 to user certificates
  - Potentially use level 4 for certificates on hardware tokens

Shibboleth

- Again as part of FAME, can acquire DNs via assertions from Shibboleth
  - These then enter the policy engine as if the client had supplied a certificate
  - LoA conditions very useful here
- Also investigating OpenID
  - very similar to Shibboleth, but with a wider take-up in the mainstream web

Summary

- Have changed internal representation of credentials to Attribute URI ("AURI") form
  – This allows easier extension of GridSite-based systems by applications / services
- Improving functionality and clarity of C API
  – GRSTx509ChainLoadCheck()
  – Logging
- LoA and Shibboleth now supported