Grid Computing: a step-by-step introduction (Day 2)

Youki Kadobayashi, Ph.D.
Associate Professor
Graduate School of Information Science,
Nara Institute of Science and Technology (NAIST), Japan

November 14, 2002 / SOI Asia

Agenda

- Grid computing = inter-domain RPC
  + resource abstraction
  + resource management
  + more features
- Namely:
  - Security features
  - Data management features
  - Some research-oriented features
- Grid standardization
- Grid operation

Security

How to transmit/receive confidential data to/from remote nodes?

- encryption of communication channels
- symmetric cipher
  - Encrypt/decrypt with shared secret
- asymmetric cipher
  - Encrypt with public key, decrypt with private key

  or
  - Encrypt with private key, decrypt with public key

How to share secret among distant nodes?

- With asymmetric cipher...
- encrypt secret (e.g., session key) with communicating peer's public key
- peer decrypts ciphertext with his private key and obtains the secret

How to disseminate public key?

- PKI (public key infrastructure)
- Digital certificate
  - (name, public key...) signed by CA
- Certificate Authority
  - A trusted entity
  - Issues certificates
- Registration Authority
  - Validates user before issuing certificate

User certificate example

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 686 (0x2ae)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=JP, O=WIDE Project, OU=members only CA
    Validity
      Not Before: Jul 11 08:07:35 2002 GMT
      Not After : Jun 30 23:59:59 2003 GMT
    Subject: C=JP, O=WIDE Project, CN=Youki Kadobayashi
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          c8:e2:f1:e1:db:2c:3a:19:9e:de:9e:43:b8:ec:d3:
          01:97:0a:fc:cf:54:f1:07:00:80:95:4b:83:41:dc
          a5:23:4f:b0:e4:4b:0c:dc:1f
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Key Usage:
        Digital Signature, Non Repudiation, KeyEncipherment, Data Encipherment , Key Agreement
      X509v3 Subject Alternative Name:
        email:youki-k @is. aist-nara .ac.j p
      X509v3 CRL Distribution Points:
        URI:http://www. moc&wide. ad.jp/crl.crl

      X509v3 Authority Key Identifier:
        keyid:56:73:3C:BA:90:02:F7:73:E9:12

  Signature Algorithm: sha1WithRSAEncryption
    26:cb:49:25:d0:1d:5b:7d:dc:07:3b:c7:0a:a3:59:a2:88:83:
    3f:d8:58:7b:e2:64:9a:35:3f:61:71:33:2b:a2:50:2f:de:a2:
    b4:94:23:19
```


CA certificate example

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 29 (0x1d)
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=JP, O=WIDE Project, CN=ROOT CA
    Validity
      Not Before: Jan 27 07:37:47 2000 GMT
      Not After : Jun 30 23:59:59 2006 GMT
    Subject: C=JP, O=WIDE Project, OU=members only CA
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (2048 bit)
        Modulus (2048 bit):
          60:db:d5:8d:e1:3f:d4:20:30:68:98:b8:6a:71:1e
          77:81:c0:fc:2b:5c:f4:e9:90:e6:c2:01:2a:14:f4 :
          b3:51
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints: critical
        CA:TRUE, pathlen:9
      X509v3 Key Usage:
        Digital Signature, Non Repudiation, KeyEncipherment, Data Encipherment , Key Agreement, Certificate Sign, CRL
  Sign
      X509v3 CRL Distribution Points:
        URI:http://www.wide.adjpwiderootcrl.crl

      X509v3 Subject Key Identifier:
        56:73:3C:BA:90:02:F7:73:E9:12
  Signature Algorithm: sha1WithRSAEncryption
    ef:08:1d:08:85:4c:78:68:62:b2:38:a4:7e:4b:31:83:31:09:
    3b:07:a8:7c:9a:33:53:22:71:25:e9:86:0e:32:02:7c:5b:98:
    32:18:71:69
```


Who is authorized to use remote computing resources?

- authentication and authorization
- global naming of user (in directory service) and global proof of user's identity (PKI's user certificate)

Single sign-on

- create a short-term, restricted certificate (credential) from user's long-term, normal certificate
- "proxy certificate"
- computation / data access are authorized with proxy certificate
- user enters password only once
  -- thus "single sign-on“

Data management

Data management questions

- how to share huge dataset among computation nodes efficiently?
- how to minimize data-access overhead without consuming excess bandwidth?

Data management strategies

- caching
- mirroring
- replica placement
  - At closest proximity...
  - Partial replica
  - Management of replica – with replica catalog
- "Data Grid" - as opposed to "Computational Grid"

More research-oriented topics

Scheduling (resource allocation / co-allocation)

- integrate diverse job-management systems
  - supercomputer's job-management systems
  - commodity computer's job-management systems (e.g., Condor)
- co-allocation:
  - simultaneous allocation of a resource set

Communication

- integrate diverse communication channels
  - TCP/IP,
  - supercomputer's vendor-specific interconnect technologies...
- Hide those diversities by providing single API for inter-node communication
- “convergence layer”

Grid application areas: functional decomposition

- data acquisition
  - Telescopes
  - Microscopes
  - ... other scientific data acquisition devices...
- data analysis
  - Wavelet transform, Fourier transform...
- Visualization
  - Graphics workstations
  - Immersive display devices (e.g., CAVE)

Grid: a research topic or useful tool?

- a research topic with growing interest
- government-funded R&D efforts in US, Europe and Asia
- Grid toolkits are mixture of many functional components
  - some are crucial
    - GridRPC , directory service, security
  - some are more research-oriented
    - data management, resource co-allocation, QoS

Grid: witness the evolution

- evolving through the iteration of:
- design - implementation - test - deployment - requirements engineering - ...
- understand technological directions of Grid
  - good for educating yourself
  - good if you are going to use it

Q&A

Step 3: Understand Grid standardization

From operating system perspective

- Grid extends key operating system features
  - resource allocation
  - user authentication and authorization
  - storage management

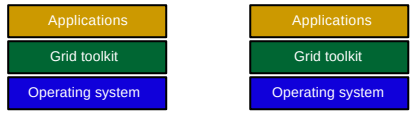
  ... beyond single administrative domain

Grid interoperability problem

- many "Grid toolkits" with different APIs, protocols...
- different programming models, operational models, functional components...

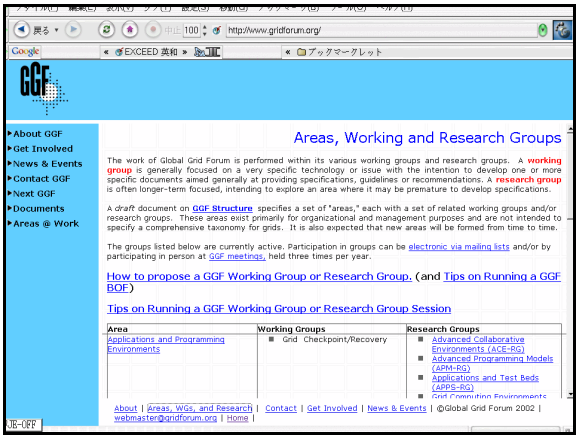
Work items for standardization

- Grid API
- Grid Protocols



GGF: global grid forum

- standardizing the Grid APIs and Protocols in the IETF way
- WGs, RGs
- www.gridforum .org



Relationship with other standard bodies

- IETF
  - SSL, LDAPv3, TCP extensions, IPv6...
- W3C
  - SOAP, XML schema, HTTP extensions...

Step 4: Understand Grid operation

Formulate your problem

- how many users are going to use your Grid?
- expected usage?
- are your users going to rewrite program?
- or do they have working code already?

Choosing Grid toolkit

- each Grid toolkit has pros and cons
- understand features and requirements of each Grid toolkit
- you may not have to choose only one toolkit
- some Grid toolkits do coexist (e.g., Globus and NetSolve)

Grid toolkit characteristics(1): NetSolve

- features:
  - simplicity
  - feasibility of deployment
  - GridRPC
- requirements:
  - single agent
  - simple rewriting of existing programs
- NetSolve - http://www.cs.utk.edu/netsolve/

Grid toolkit characteristics(2): Globus

- features:
  - multi-institutional directory service
  - multi-institutional user identification
  - multi-institutional authentication and authorization
  - integration of MPI and other legacy supercomputing tools
- requirements:
  - directory server
  - Certificate Authority (if you want confined Grid)
- Globus - http://www.globus.org/

APGrid

- Open coalition of Grid-ready institutions in AP
- 15 countries, 41 institutions
- http://www.apgrid.org/

Summary

- Grid: distributed computing re-architected
  - IETF/W3C-defined protocols as building blocks
    - SSL, LDAP, Kerberos, TCP/IP...
  - Oriented toward the scale of the Internet
    - Delay/performance variability, policy awareness...
  - Living examples of latest Internet standards
    - PKI, LDAPv3, etc.
- Grid toolkit: aggregate of middleware
  - Variety of choices - you can start small
- Opportunities of participation & contribution