Security Issues in Grid Computing

Presented by:
Nisarg Gandhi
Aritra Mukherjee
Anirudh Sethi
Abstract

• Secure management of Grid systems presents many challenges.

• This paper examines the security requirements that are essential to Grids and some of the software that is available to meet them.

• We discuss how well these security mechanisms have been utilized and review some of the existing and proposed security standards that may be the foundations of the next generation of Grid security.

• We expose some weaknesses in existing systems and we suggest some techniques and methods which will help enhance the grid security.
Introduction to Grid Computing and Grid Security

• Grid is a massively huge network of computers
• Grid computing is application of several computers to a single problem at the same time
• Examples of Grids are SETI@Home, World Community Grid.
• Grid Security has Architecture, Infrastructure and Management issues
IMPORTANCE OF GRID COMPUTING

• Offers less expensive alternative to purchasing new, larger server platforms.
• Sometimes workload requirements exceed existing server platform capabilities.
• Useful for small tasks like movie rendering to solving huge computational problems of future.
• Future infrastructure.
SECURITY ISSUES IN GRID COMPUTING

Grid Security Issues

Architecture Issues
- Info. Authorization
  - Secure Comm.
  - Authentication
  - SSO & Delegation
- Services
  - VO Level
- Host
  - DoS
  - QoS Violation
  - Job Starvation

Infrastructure Issues
- Network
  - Data Protection
  - Access Control
  - Routing
  - Sensor Grid
  - Multicasting
  - High Perf.
- Cred. Mgmt
  - Repositories
- Trust Monitoring
  - Trust Creation
  - Trust Nego
  - Grid Level

Management Issues
- Trust Mgmt
ARCHITECTURE ISSUES

- Grid should protect flow of information to trusted parties
- User’s Data should be protected
- User’s personal data and system data should be distinguished
- Resource level authorization
- Delegation of Identity and Single Sign On
INFRASTRUCTURE ISSUES

- Issues related to network and host components
- Host Issues-prevention of misuse of user’s data and resources
- Prioritizing local jobs over system jobs
- Job Starvation
- Availability
- Multicasting, traffic censoring are issues to be handled
MANAGEMENT ISSUES

• Scheduling, Rescheduling.
• Monitoring, Auditing and Logging
• Host and network component compatibility
• Management is difficult due to heterogeneous nature of the Grid.
• Routing
OTHER ISSUES

• Assurance Mechanisms are seldom used in Grids
• Accounting-required to assist Auditing mechanism
• Auditing- essential to monitor system performance
PRESENT SECURITY MEASURES

• Authentication
• Authorizing
• Intrusion Detection
• Cryptography
• Virtual Private Networks
• Firewalls
AUTHENTICATION

• Process of verifying identity of a participant to an operation or request
• Principal: entity whose identity is verified
• Local user OR user logged into remote system
• Traditional systems: Authenticate client to protect server
• Grid systems: Mutual Authentication required
• Ensure that resources and data not provided by an attacker
Authentication Methods: Password-based Authentication

- Send unencrypted passwords: only suitable when messages can’t be read by
- Untrusted processes while on network
- Instead: Prove knowledge of a password: Don’t send password over network
- Use password as an encryption key
- Encrypt a known but non-repeating value
- Send encrypted value to party verifying authentication
- Both parties must know password or trust a third-party to distribute it
Authentication Systems: Kerberos

- Authentication and key distribution Protocol
- Used with symmetric encryption systems
- Better performance than systems using public key or asymmetric cryptography
- Well-suited to frequent authentication
- Centrally administered
- Requires trusted, on-line Certification Authority: Key Distribution Center (KDC)
Authentication Systems: Secure Sockets Layer (SSL)

- Widely-deployed in every web browser
- Client authenticates identity of the server
- Send a session key from client to server to set up an encrypted communication
- Server has a certificate that contains its public key
- If client has a certificate, can authenticate itself to the server
Certificates and Certification Authorities (CA)

• Certification mechanism provides binding between encryption key and authenticated identity
• Certification authority (CA) is a third party that certifies or validates the binding
• CA issues a certificate and signs it
• Certificate is a data object that contains:
  o Distinguished name of a principal
  o In asymmetric cryptographic systems: the public key of the principal
  o Optional attributes: authorizations, group memberships, email addresses, alternate names
AUTHORIZATION

• Process that determines whether a particular operation is allowed
• Traditionally: based on authenticated identity of requester and local information
• Grids: determine whether access to resource is allowed
  o Might have access control lists associated with resources, principals or authorized programs
  o User-provided code must also be authenticated
INTRUSION DETECTION

- Keeps track of network activity
- Checks ports and protocols for possible attack
- Generates an alarm when finds an anomaly
- Generally does not work on Grids, most Grid applications appear as threats and generates false alarms.
CRYPTOGRAPHY

• Symmetric and Asymmetric cryptography is used
• Used for authentication as well as communication
• Users, resources and applications need to be authenticated.
• Algorithms used-DES, RSA
VPNs and Firewalls

- VPNs are used in Grid Security at transport layer
- Confidentiality and Integrity
- Firewalls serve between two networks
SECURITY MEASURES ASSESSMENT AND IMPROVEMENT

- Authentication should be done each time a user enters a Grid
- Passwords should be encrypted
- Common third party for key distribution must be agreed when using Kerberos
- Focus should be on user authentication not only server authentication
- Newer schemes based on ACLs should be configured
- Standard algorithms should be backed by using algorithms like PGP
DEMONSTRATION
CONCLUSION

• Few issues in Grid Security have to be tackled differently
• Lot of resources and users will become a part of the Grid in the future
• Need to be prepared to tackle all kinds of threats
THANK YOU
REFERENCES

- A taxonomy of Data Grids for distributed data sharing, management, and processing - Srikumar Venugopal, Rajkumar Buyya, Kotagiri Ramamohanarao
- Proceedings of the 5th international workshop on Middleware for grid computing: held at the ACM/IFIP/USENIX 8th International Middleware Conference: held at the ACM/IFIP/USENIX 8th International Middleware Conference - Bruno Schulze, Omer Rana, Jim Myers, Walfredo Cirne
- Proceedings of the 4th international workshop on Middleware for grid computing - Bruno Schulze, David Abramson, Radha Nandkumar, Rajkumar Buyya
- Proceedings of the 5th IEEE workshop on Challenges of large applications in distributed environments - Jennifer M. Schopf, Raymond Bair, Nancy Wilkins-Diehr, Sergiu Sanielevici
- The Grid in a Nutshell - Ian Foster and Carl Kesselman
- Scheduling in the Grid Application Development Software Project - Holly Dail, Otto Sievert, Fran Berman, Henri Casanova, Asim Yarkhan, Sathish Vadhiyar, Jack Dongarra, Chuang Liu, Lingyun Yang, Dave Angulo, and Ian Foster
- Grid Resource Management in Legion - Anand Natrajan, Marty A. Humphrey, and Andrew S. Grimshaw
- Grid Scheduling with Maui/Silver and David B. Jackson
- Using PredictedVariance for Conservative Scheduling on Shared Resources - Jennifer M. Schopf and Lingyun Yang
- Improving Resource Selection and Scheduling Using Predictions - Warren Smith