

GARUDA Security: Issues and Approaches

CNIE Division
C-DAC, Electronics City
Bangalore



Agenda

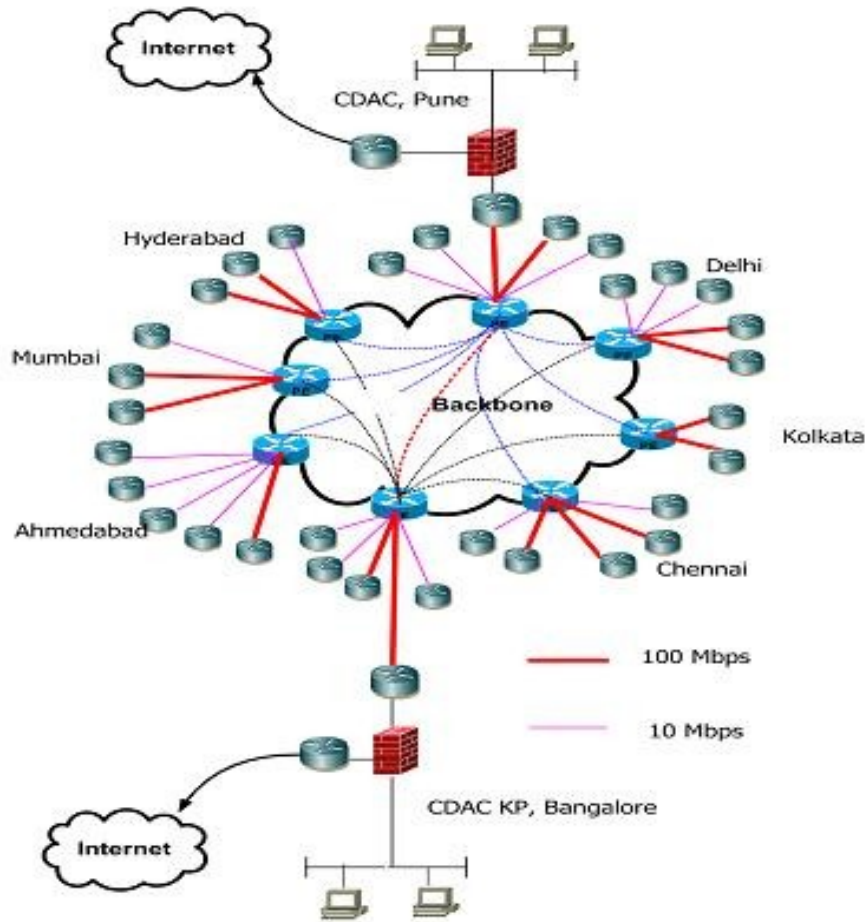
- Need
- Architectural Elements
- Middleware Elements
- Vulnerabilities and Exploits in GARUDA
- Challenges
- R&D
- Approaches
- Demo



Need for Security

- Grid Computing: Multiple administrative domains sharing resources
- Requirements of awareness creation amongst different Grid communities working on applications, middleware, architecture and resource management
- Building a common team across the grid community to address security issues is very much essential as “no single agency can take ownership of the entire GARUDA grid”
- Requirements of Confidentiality, Integrity, Availability, Physical Security, Access control and Traceability
- Grid environment: More controlled, awareness of security risks and proper planning can make grid computing safe

GARUDA: A Grid Computing Initiative (Module 1 Cities)



Architectural Elements

- Wide-area Communication Fabric:
 - L3 MPLS VPNs and L2 fallback between C-DAC Blr and Pune
 - Firewalls protection for C-DAC Resources
 - PKI
 - Private IP Addresses (10.x.x.x)
 - *Multiple parties involved (C-DAC, ERNET, ISP(s) and Partner Institutes)*



Security Issues

- **VPN:** VPNs shall provide encryption to data during the transit but they do not provide undetectability of activities
- Possibility of interconnecting GARUDA and Internet at any site
- Firewall Issues: Proper analysis application requirements yet to be carried out to freeze controls using firewall (assuming firewall is present at multiple levels)
- Traffic Flow: Study and understanding for Traffic flows to be carried out to arrive tighten the security
- PKI: Issues related to Automatic Trust Decisions
- Heterogeneous Resources : Vulnerable OS, Services and Applications

Middleware Elements

- GARUDA implements Globus version 2.4
- Certifying Authority using Simple CA managed by C-DAC
- Job submission through portal and command line modes
- Provisions for executing native commands



Security Issues

- **Job Submissions:** security concerns in case of the command line option that can exploit using commands of the native OS executables
- **PKI:** Issues related to cross certifications and deciding trusted CAs.

S.No	Command	Threat
1	<code>grid-job-run gridhost /bin/cat /etc/passwd</code>	Reveals user information hence using a passwd cracking utility passwd can be cracked
2	<code>grid-job-run gridhost /bin/cat /etc/hosts</code>	Reveals the Grid headnodes information such as IP address and host names
3	<code>grid-job-run gridhost /bin/cat /etc/sysconfig/network</code>	Reveals the Gateway address after which DoS can be attempted

S.No	Command	Threat
1	<code>globus-job-run gridhost /usr/bin/poweroff.</code>	A grid user (unprivileged) can shut-down the system remotely
2	<code>globus-job-run gridhost /usr/bin/reboot</code>	A grid user (unprivileged) can reboot the system remotely
3	<code>globus-job-run gridhost /usr/bin/uname</code>	A grid user (unprivileged) can know details of the system



Vulnerabilities & Exploits

- Carried out certain probing and security analysis at various nodes
- Carried out experimental TCP Syn flood, ICMP Flood, Buffer overflows, Port scanning
- Attempted various commands from globus environment to gain more information and insights about remote nodes
- For details: Refer our paper “GARUDA Grid Security Analysis - Issues and Approaches”

Challenges

- The Complexity that exists in a grid environment due to heterogeneous resources
- Difficulty in evolving and enforcing security process, procedures and policies
- Security is a on-going routine activity and not a onetime activity
- Developing solutions for many grid specific protocols, applications and middleware

Research & Development

- Grid Traffic flow analysis
- Simulations of security (OptorSim, ChicagoSim, Simgrid, Gridnet...)
- Policy based Security framework (Policy specification language - ASL, ISPS, KAoS, LaSCO, PCIM, PDL, PMAC, PPL..)
- Secure Programming and application security
- Grid specific security solutions
- Virtual community specific security solutions
- Threat & Attack Modeling, Attack prediction and mitigation
- Development of Managed Security Solutions
- Self-healing and immune architectures
- Cyber (Grid) Forensics
-

Approaches and CALL for Participation

GARUDA Security Policy

- Evolving Security practice statements and GARUDA Security Policies
 - Evolve responsibilities for Resource Providers as well as users
 - Carryout risk assessment and fix the weakness
 - Form a Group to evolve Policies
- Participation in International Grid Trust Federation (IGTF), established October 2005 (<http://www.gridpma.org/>)
 - **Asia Pacific Grid PMA**
 - **European Grid PMA**
 - **The Americas Grid PMA**
- Asia Pacific Grid Policy Management Authority (APGrid PMA)

GARUDA – CERT (G-CERT)

- URGENT need of the Hour: GARUDA – Computer Emergency Response TEAM **(G-CERT)**
 - To be a Collaborative effort by all/many partners (SSO at each site)
 - To establish points of trusted contacts for computer security threats in GARUDA
 - To provide certain mandatory services like IR, Announcements, vulnerability analysis, technical analysis and reports, education, incident tracing, intrusion detection, audits and penetration testing, security consultancy, risk analysis etc.,
 - Create documents pertaining to Best practices and policy guidelines (site security and inter-site security handbook)
 - Create awareness by conducting short-term courses, workshops and seminars
 - Announcement and advisories (Early warning)
 - To develop capabilities to support activities such as tracking and tracing intruder activity and active detection of such activities
 - Interface with CERT-IN and other CERTs

CDAC's Questionnaire on G-CERT INITIATIVE

- To form the collaborative Incidence Response Team
- In case if you are not directly involved in security related aspects, you may pl. nominate/mention a suitable person from your Organization
 - Use the last question.5 (comments / feedback for this purpose)
- C-DAC has expertise in Cyber Security across various centers

Standardization Bodies

- ISO/IEC - Wide scope of coverage, focusing on standardization, more general framework. 17799-1 and 13335 most relevant
- IETF - Focuses on Internet related technical Security requirements
- NIST-CSRC (<http://www.nist.gov/>) - Wide scope of coverage for both government and enterprise needs. Many relevant documents that can be leveraged
- OASIS (<http://www.oasis-open.org/>) - Application Vulnerability Description Language (AVDL)
- OGSF (Open Group Security Forum, <http://www.opengroup.org/security/>) - specifications, tools, guidelines and best practices for businesses, responsibilities, liabilities and trust relationships; started Intrusion Attack and Response Workshop

Best practices and recommendations

- CERT/CC (<http://www.cert.org/>) - a center of Internet security expertise; recommendations, advisories, practices, research
- SANS (System Administration, Networking, and Security) Institute - <http://www.sans.org/>, focuses on SysAdmin, Audit, Network, and Security research and education.
- ISACA (<http://www.isaca.org/>) - Most noted for CoBIT, provides a comprehensive framework for IT Governance, including security
- ISSA (<http://www.issa.org/>) - comprehensive coverage of security issues and solutions for InfoSec practitioners, GAISP (Generally Accepted Information Security Principles)

Working Groups and Documents

- GRIP (concluded) - Guidelines and Recommendations for Security Incident Processing
- IDMEF (concluded) - Intrusion Detection Message Exchange Format
- INCH - Extended Incident Handling WG
(<http://www.ietf.org/html.charters/inch-charter.html>)
 - IODEF and RID development
- OPSEC - Operational Security Requirements (OPSEC) Working Group
 - Requirements to secure deployment and operation of managed network elements at OSI layers 2 and 3; targets ISP's and vendors
- RFC 3552 - Guidelines for Writing RFC Text on Security Considerations
 - Discusses Internet threat model, including active and passive attacks, DoS
 - RFCs: 2196, 2350, 2505, 3013, 3227, 2828
- GGF: OGSA Security Working Group

Global Initiatives

- EGEE – Enabling Grids for E-science
 - JRA3 – Security
 - MWSG – Middleware Security Group
 - JSPG – Joint with LCG and OSG Security Policy Group
 - OSG Incident Handling Activity
- Recent Security related deliverables
 - Grid User/Site Security Requirements – MJRA3.1 (<https://edms.cern.ch/document/485295/1>)
 - Global Security Architecture (GSA) rev. 1 - DJRA3.1 (<https://edms.cern.ch/document/487004/1.1>)
 - Grid Security Incident definition and exchange format – MJRA3.4
 - Ongoing development, current version - <https://edms.cern.ch/document/501422/1>
 - As a part of joint OSG/LCG/EGEE Operational Security activity
- Grid Security Incident (GSIInc)
- NIST-CSRC (<http://csrc.nist.gov/publications/nistpubs/>)

DEMO

C-DAC's N@G & INetTalk