

# Grid Security: Survey, Analysis and Research Directions



CNIE

## GARUDA Partner Meet

**Subramanian N**  
C-DAC, Electronics City  
Bangalore

4<sup>th</sup> March 2008

# AGENDA



CNIE

- Grid Security Need
- Internet Security Vs Grid Security
- Grid Security Analysis
- Research Challenges
- C-DAC Initiatives
- Conclusion

# Need

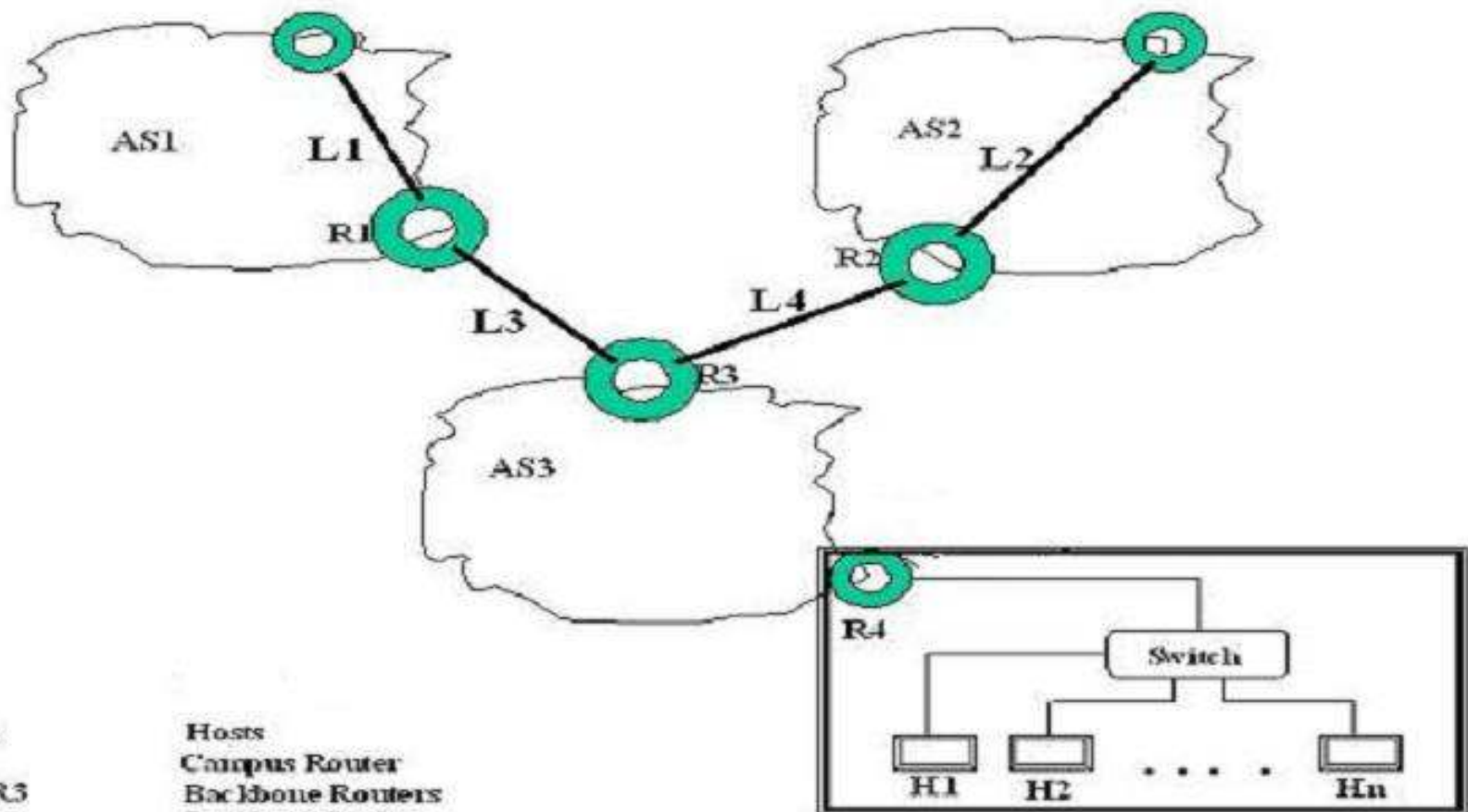


CNIE

- Security Elements: Access control, Availability, Confidentiality, Integrity, Physical Security, and Traceability
- Secure sharing: Multiple administrative domains sharing resources
- Secure environment: Cooperation and coordination amongst all grid nodes to evolve safe environment
- Large Users and resource's unpredictable and dynamic at any point
- Different organizations which do not have trust agreements
- Interactions between services and services acting on behalf of users

# Typical Network Scenario

Network Scenario



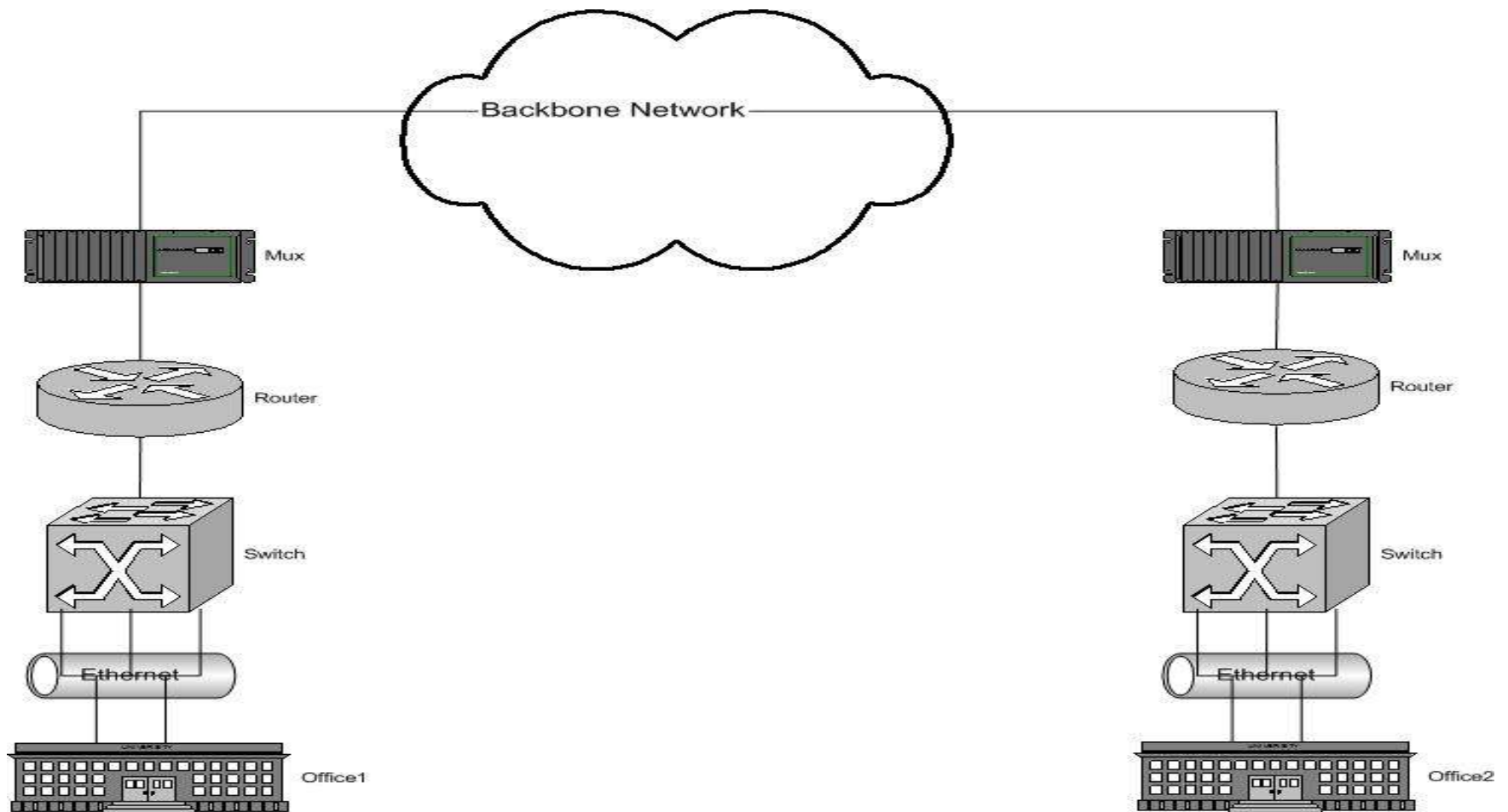
H1, H2, ..., Hn  
R4  
R1, R2 and R3  
L1, L2, L3, L4  
AS1, AS2, AS3, AS4

Hosts  
Campus Router  
Backbone Routers  
Backbone Links  
Autonomous System

# End Nodes



CNIE



# Internet Vs Grid security



CNIE

- Policy based management
  - Loose in Internet
- Configuration Management
  - Device, protocols, software and applications
- Applications
  - Well-known in internet
- Data Flow
  - Replication/QoS/Volume/Periodicity...

# Internet Vs Grid security



CNIE

- Network Perimeter
  - Public and Private networks
  - Perimeter security
- Middleware services
  - PKI
  - Job Scheduling
  - Grid monitoring and management
- Transport Layer Issues
  - One-way SSL and Two-way SSL

# Common Security Issues



CNIE

- DoS, DDoS
- Buffer overflows
- Gaining privilege
- Worm
- Data theft
- Information gathering
- Flooding attacks

# Grid Security Analysis



CNIE

# Can Any thing worst happen ?



- Attacks against new Grid components..
- High compute resources..(DoS..)
  - Junk program/data consuming resources..
  - *'A grid is an automated error amplifier' (D.Skow)..*
- Grid applications behavior
- Is it possible to profile normalcy of traffic
  - Like bimodal distribution nature..??
- Target schedulers..

# Ok is there any good news?



CNIE

- Well,
  - PKI framework
  - Formal MoUs between agencies (management level understanding)
  - Hence enforcing technical configurations..possibly easy..
  - Common policy and standardization

# Common Security Solutions



CNIE

- Firewall
- IDS & IPS
- Anti-virus
- PKI
- Encryption boxes
- Authentication and Access control

# Are they applicable?



- Yes +
- Automatic threat assessment
- Adaptive and Dynamic Firewall
- New techniques for identifying intrusions
- Dynamic configuration facilities
- User, Resource, Flow, Scheduler, Application profilers..
- Enhanced Audit capabilities
- Vigilance, monitoring and patrolling agents

# State of Art



CNIE

- Good progress in middleware framework for authentication and authorization
- Evolving Standardization initiatives such as Grid Trust Federation that establishes the Policy management authorities
- Security Operations : to be streamlined and automated..
- Control points for Policy framing, policy enforcement, monitoring and forensics : to be strengthened further..

# Research Challenges



CNIE

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

# C-DAC's Initiatives



CNIE

- Adaptive Firewall
  - Objective: To devise a dynamic configurable firewall for grid environment
- Self-Management
  - Objective: To devise mechanisms towards self-configuration of network entities
- Authentication
  - Image based multi-factor authentication mechanisms

# Standardization Bodies



CNIE

- 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



CNIE

- 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



CNIE

- EGEE – Enabling Grids for E-scienceE
  - JRA3 – Security
  - MWSG – Middleware Security Group
  - JSPG – Joint with LCG and OSG Security Policy Group
    - OSG Incident Handling Activity
- 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/>)

# Key References



CNIE

- EGEE security initiatives
- Globus Security Model for Grid environment, Nitin V. Kanaskar, Umit Topaloglu, Coskun Bayrak, ACM SIGSOFT Software Engineering notes



CNIE

# Thank You!!