Security at Scale

LEADERSHIP COMPUTING FACILITY
NATIONAL CENTER FOR COMPUTATIONAL SCIENCES

presented by
David Vasil

DOE Exascale Town Hall
May 18th, 2007

Oak Ridge National Laboratory
U.S. Department of Energy

Goals for Confidentiality/Integrity/Availability (CIA) at Scale

- Confidentiality
  - Large scale data encryption
  - Removal of remnants
  - System partitioning
- Integrity
  - Checksums of large amounts of data
  - Checksums of data from end-to-end
  - Verifiable systems
- Availability
  - Redundancy throughout the system
  - Containment of incidents
  - Quickly react to events
  - Maintain data utility

Two competing needs

- Science
  - Provide results *now*
  - Share information
  - Interconnect
  - Bleeding edge
  - Unattended authentication
  - Users from outside orgs
- Security
  - Validation
  - Restrict information flow
  - Restrict connections
  - Verified system configuration
  - Strong authentication
  - Tightly controlled user base

Solutions for Security at Scale

- Current activities
  - Thin nodes
  - Host integrity verification
  - One-time passwords
  - Network partitioning
  - Event correlation

- Future concerns
  - Lightweight and hardened systems
  - Secure interconnects
  - Anomaly detection of user activity
  - Anomaly detection of process activity
  - Distributed checksums
  - Event correlation with active response

Possible Areas of Research for Security at the Exascale

- Large scale data integrity verification
- Determining whether a process or user is acting out of scope
- Tools for monitoring the health and security of large scale distributed systems
- Tools to quickly contain, repair, and analyze compromised clustered systems