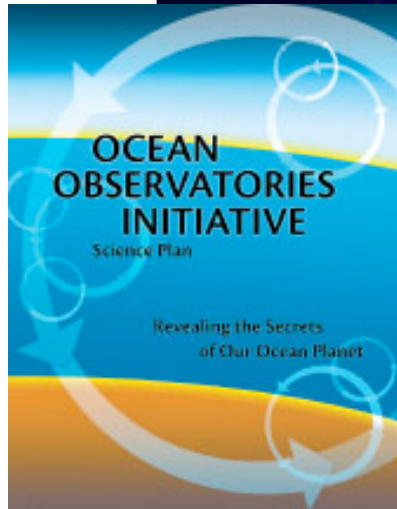
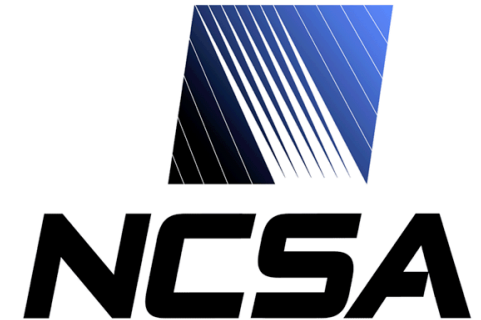


# Security for High-end CyberInfrastructure: Lessons Learned

Randy Butler, Roy Campbell,  
Himanshu Khurana, Adam Slagell, Von Welch  
National Center for Supercomputing Applications  
and  
Information Trust Institute  
University of Illinois

# Lessons Learned from...



**Open Science Grid**

Worldwide LHC Computing Grid  
Distributed Production Environment for Physics data Processing



GENI Security Workshop (Jan 2009)

Von Welch <[vwelch@ncsa.uiuc.edu](mailto:vwelch@ncsa.uiuc.edu)>

# GENI and previous CI

- Some key differences.
  - Heavy use of VLANs and VMs.
  - Jobs are more "experimental" and "deeper" in nature.
    - e.g., the networking infrastructure itself is open to experimentation
- Many similar challenges and goals.
  - Multiple, distributed organizations.
  - Distributed user community.
  - Availability and Integrity of resources.
  - Keeping user "jobs" isolated.

## Some Lessons GENI Can Build On

- Your biggest security problems are the ones you don't own.
- The hackers don't care about your software.
  - The hackers don't take the time to read the manual either.
  - It's all the usual stuff - Password theft, scans getting lucky, PHP, MySQL, kernel vulnerabilities, etc.
  - So far... the day may come, but it has been "coming" for a while.
- End user workstations are the biggest entry point for attacks.

# Lessons

- Preparation and planning for incident response is critical.
  - Flowcharts.
  - Dry-runs and exercises.
  - Make sure you are doing the right logging and auditing.
- Plan for collaboration during an incident.
  - How will responders communicate with each other?
  - Who communicates with media? NSF? Users?
  - How do responders securely share data, correlate events, etc.

# Lessons

- Getting agreement on security issues is hard
  - Need to include all the stakeholders.
  - Inevitably someone will have a problem with everything.
- Other Issues:
  - Handling software vulnerabilities is a constant distraction.
  - Don't underestimate value of training.
    - Of users, administrators and management.
  - Centralization versus decentralization of control.
    - Often move to the former as trust grows.

# Opportunities with Virtualization

- VMs:
  - Better job isolation and lower level monitoring.
  - Can suspend and capture suspicious jobs.
- VLANs:
  - Better isolation of job traffic from “Internet background noise” allowing for better IDS through reduced false positives.
- All require tighter integration of security tools with VM/VLAN technologies than is typical today.

Thank You.



GENI Security Workshop (Jan 2009)

Von Welch <[vwelch@ncsa.uiuc.edu](mailto:vwelch@ncsa.uiuc.edu)>