

Protecting the Information Technology Infrastructure

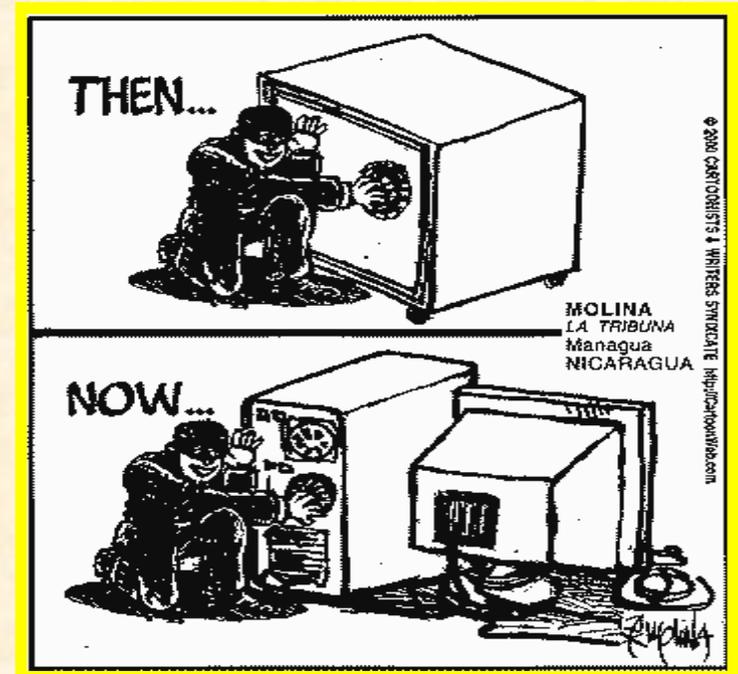
E3SGS Town Hall Meeting

Cybersecurity Breakout

May 18, 2007

B4: Cybersecurity Breakout

- **Develop tools and methods to protect the distributed information technology infrastructure**
 - ensuring network security
 - preventing disruption of our infrastructure
 - defend distributed systems against attack



B4: Cybersecurity Breakout

- **Support of cybersecurity situational awareness (SitAware)**
- **Modeling of human and application behavior**
- **Provide service oriented capabilities**
- **For each of the above**
 - **What is state-of-the-art?**
 - **What are the challenges?**
 - **What is plausible to achieve in 5-10 years?**

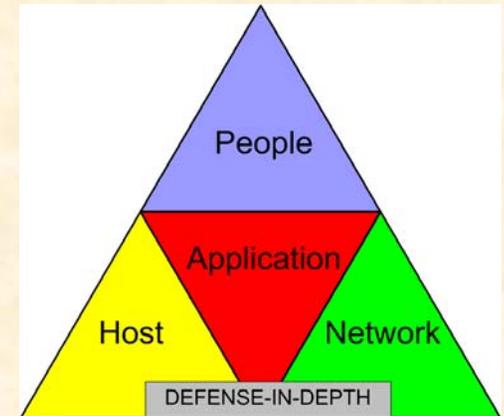
The Future at the Exascale

- **Unprecedented scale and complexity**
- **Diverse and global user population**
- **Extensive Portals to resources for communities of users**
- **Storage and retrieval of large datasets and data collections**
- **Complex user credential environment to support collaborations and virtual organizations**
- **Expected evolutionary change in security tools**
- **Anticipate the revolutionary change in cybersecurity**

Cybersecurity Today and Future

- **Today**

- Terascale and Petascale
- Large distributed data collections
- Defense in Depth
- Automated security analysis of individual component or their logs
- Anomaly and intrusion detection (NIDS and HIDS)



- **Future**

- Petascale and Exascale
- Data and data collection integrity assurance
- (*what is future security model? DRM? Other?*)
- User behavior characterization for anomaly detection
- Powerful indexing and search of log aggregates

Cybersecurity Breakout Goals

- **Panel discussion format with time for open discussion**
- **Generate cybersecurity requirements**
- **Definition of state-of-the-art and futures**
- **Identify gaps or bottlenecks**
- **Identification of research programs to address the cyber security gaps**