# Design Deployment and Use of the DETER Testbed

**Terry Benzel, Robert Braden, Dongho Kim, Clifford Neuman Anthony Joseph, Keith Sklower, Ron Ostrenga, Stephen Schwab**

Clifford Neuman

Director, USC Center for Computer Systems Security

http://clifford.neuman.name

USC Viterbi School of Engineering

Berkeley University of California

SPARTA

UNIVERSITY OF SOUTHERN CALIFORNIA
INFORMATION SCIENCES INSTITUTE

DETER Community Workshop on Cyber Security and Test

August 6, 2007

Boston

# The DETER Vision

… ***to provide the scientific knowledge required to enable the development of solutions to cyber security problems of international importance***

**Through the creation of an experimental infrastructure network -- networks, tools, methodologies, and supporting processes -- to support experimentation on research and advanced development of security technologies.**

# DETER Testbed Goals

- **Facilitate scientific experimentation**
- **Establish baseline for validation of new approaches**
- **To protect the public internet from the side effects of security experiments**
  - Saturated Links
  - Broken routing
  - Exfiltration of malicious code
- **Provide access for wide community of users**

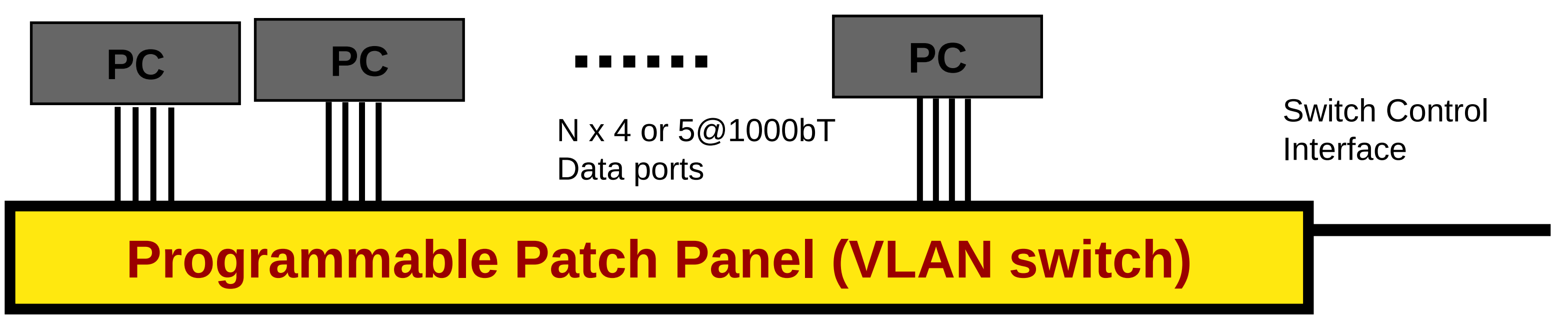
# The DETER Testbed Provides

- **Fidelity: Realism of environment**
  - Number and kinds of nodes, services
- **Repeatability: Controlled experiments**
  - Can be rerun, varying only desired characteristics.
  - Unlike the real internet
- **Programmability: Ability to modify algorithms**
  - To test new things.
- **Scalability: Ability to add more nodes**
  - Multiple clusters
  - Virtualizations
- **Isolation and containment**
  - Protects experiment and protects others

# The DETER Experimental Network is Based on Emulab

Cluster of N nearly identical experimental nodes, interconnected dynamically into arbitrary topologies using VLAN switches.

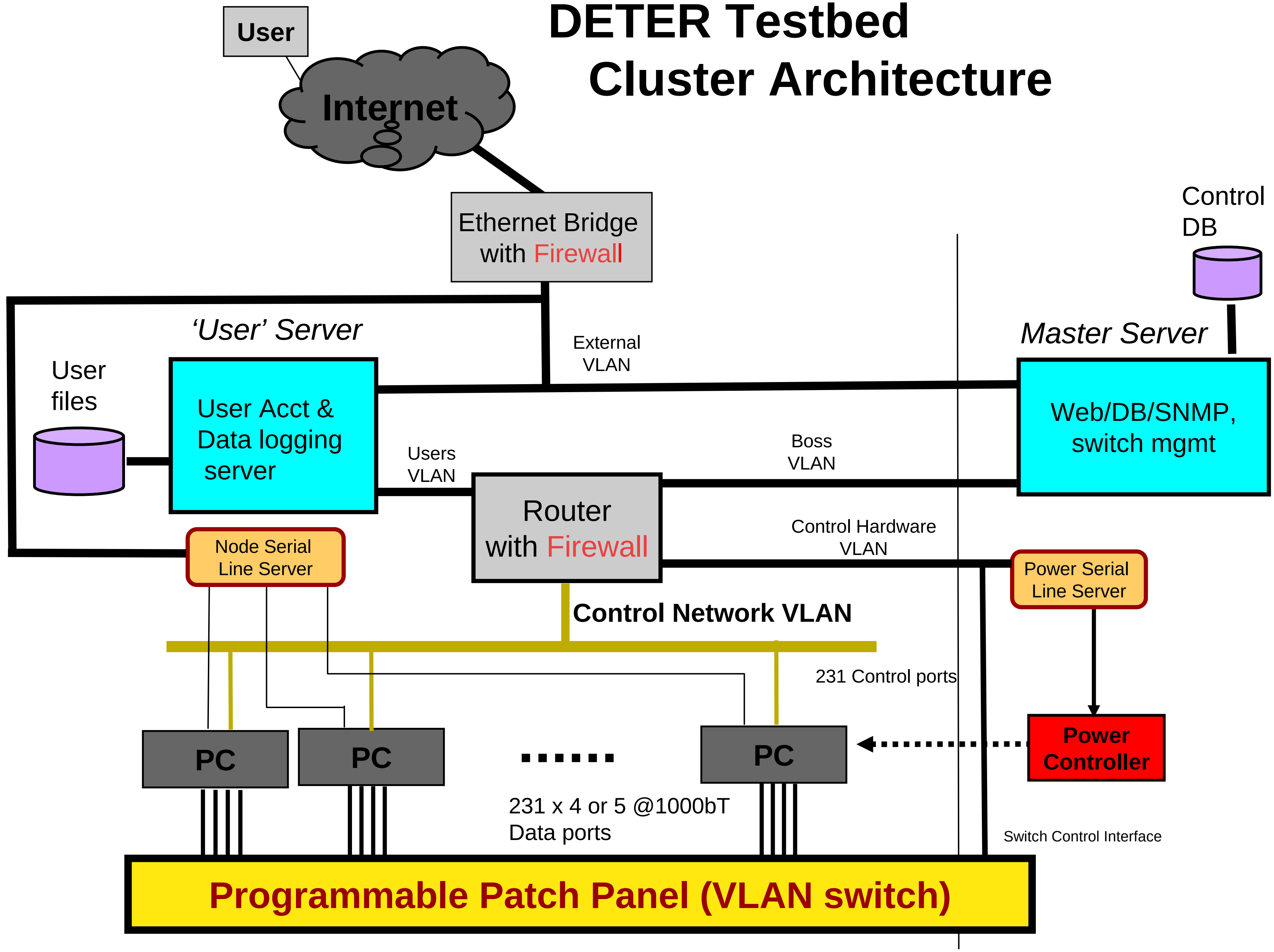
**Pool of N processors**



# The DETER Architecture

- **Emulation cluster based upon University of Utah's Emulab**
  - Basically homogeneous
  - In some cases we have integrated experimenter specific nodes.
    - Controlled hardware heterogeneity
    - Specialized Devices including Routers, ID systems, etc.
- **Implements network services – DNS, BGP**
- **Provides containment, security, & usability**

# DETER Testbed Cluster Architecture



# Interconnecting Clusters

**Two clusters: USC -ISI, UCB**

**One control site (ISI)**

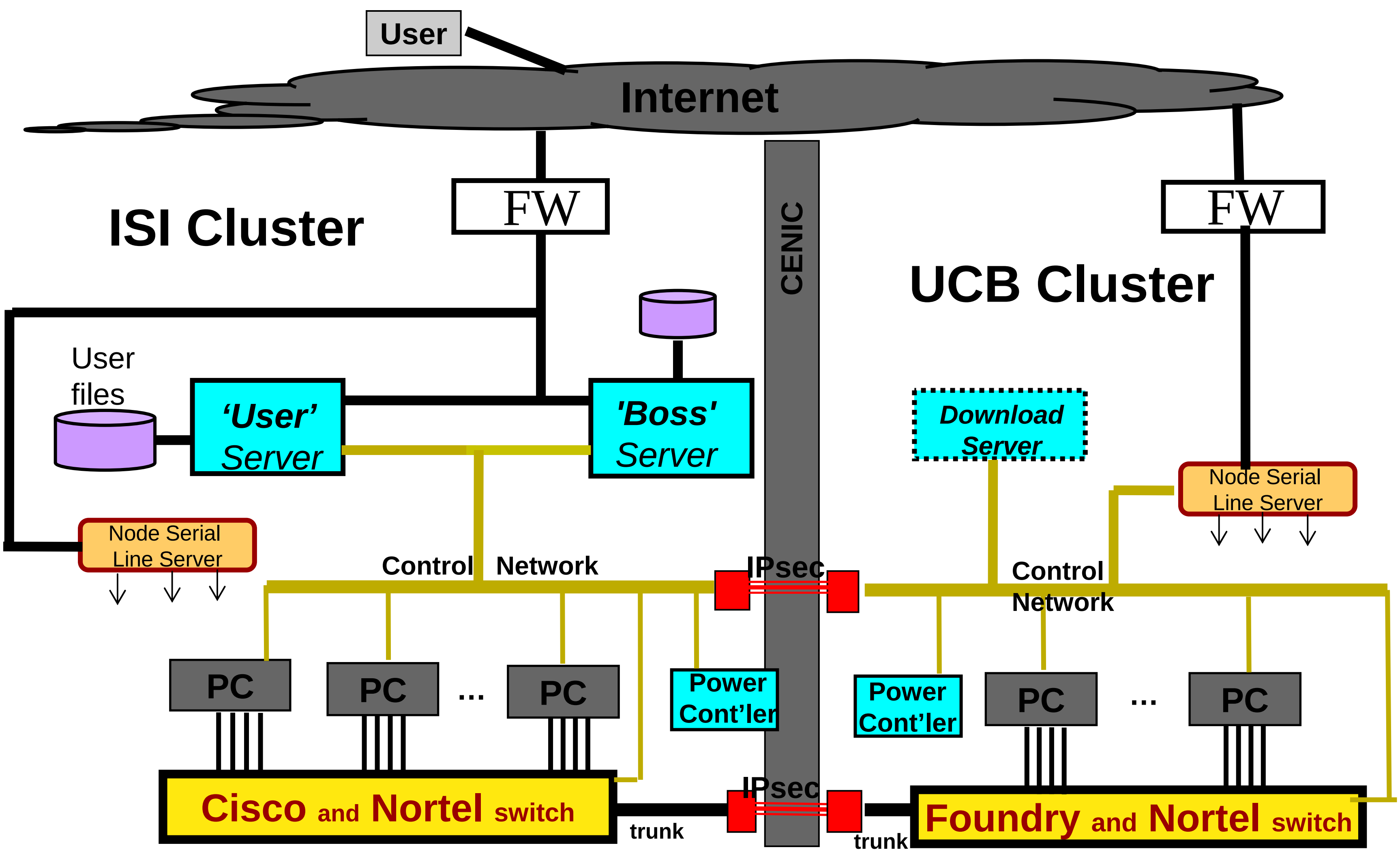
- One user entry point, accounts, control

**Connection**

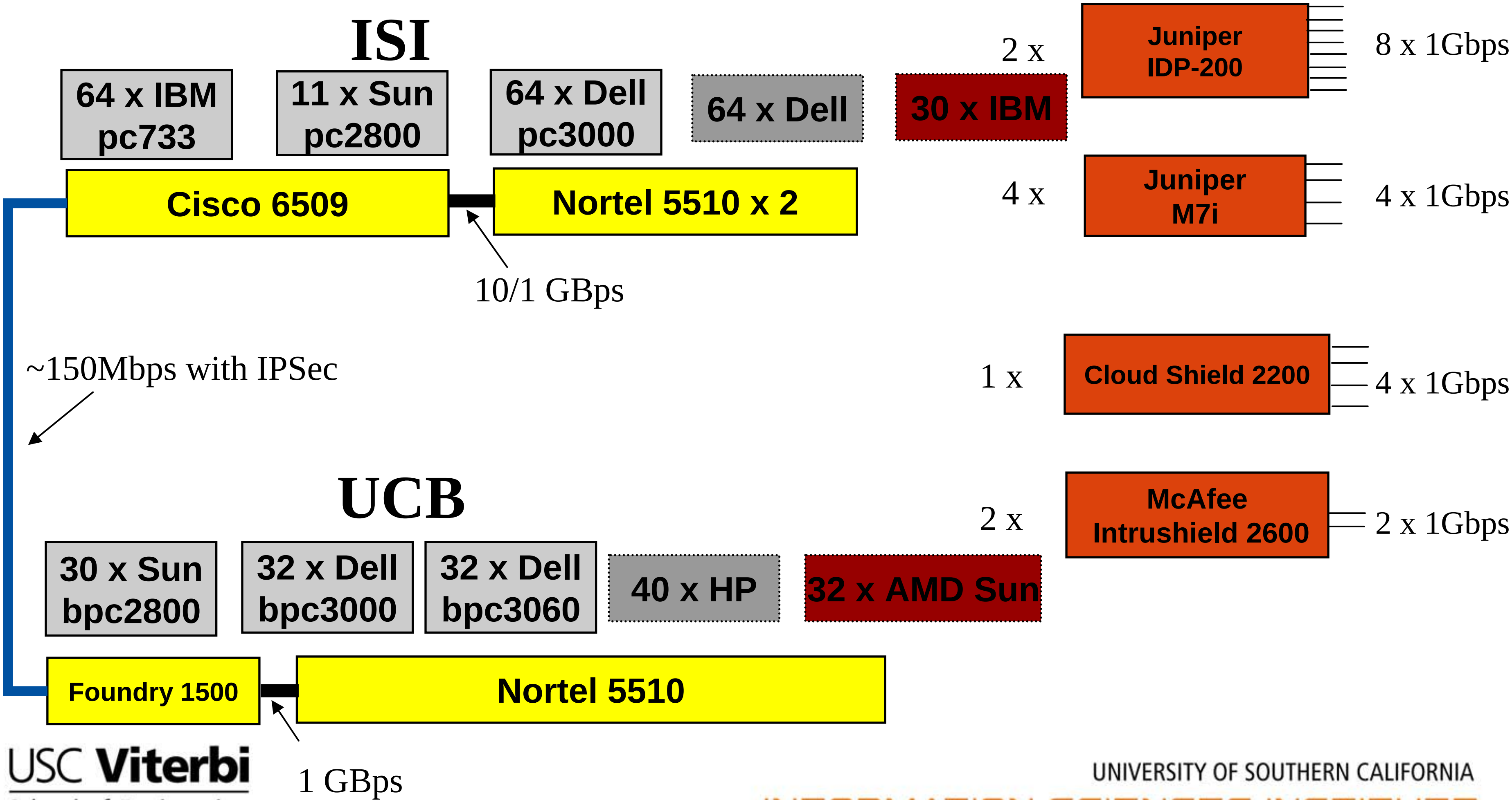
- CENIC: CalREN-HPR

**VLAN switches interconnected using proprietary layer 2 tunnels**

- Form one pool of nodes to be allocated
- User can control whether span multiple clusters
- The tunnels may be encrypted using IPSec


User
Internet
FW
FW
ISI Cluster
CENIC
UCB Cluster
User
files
'User'
Server
'Boss'
Server
Download
Server
Node Serial
Line Server
Node Serial
Line Server
Control Network
IPsec
Control
Network
PC
PC
...
PC
Power
Cont'ler
Power
Cont'ler
PC
...
PC
IPsec
Cisco and Nortel switch
trunk
trunk
Foundry and Nortel switch

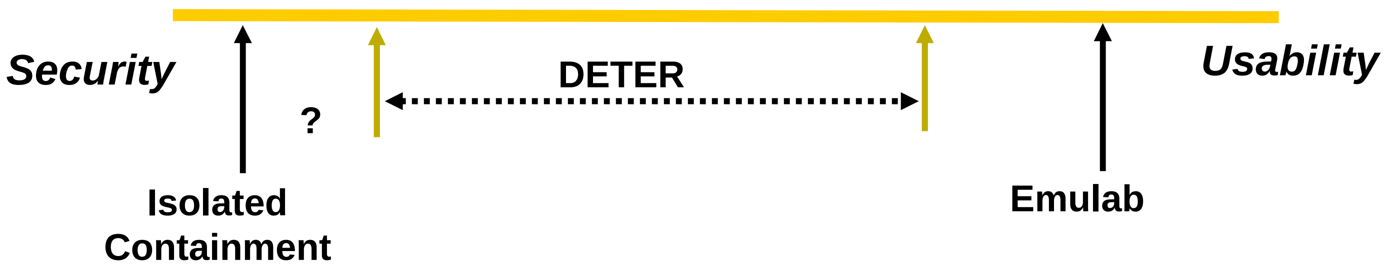
# DETER Hardware Status



# Handling Scary Code

## Objective: Variable-safety testbed

- Adaptable to threat level of experiment
- Supports shared, remote experimenter access for low-threat code; varying degrees of isolation.
- *Research question: can we design DETER to safely handle the entire range of threats, or will really scary stuff have to run in some other isolated containment facility?*



# Security is Critical

- **Security must be balanced with needs of researchers**
  - Defenses employed by the test-bed must balance the requirements of containment, isolation, and confidentiality, with the need for remote management of experiments.

- **Possible consequences of breach are considered**
  - Experiments are categorized according to the consequences of loss of containment, and procedures applied according to that categorization.

# Achieving Security

## Operational

- Procedures for proposing and reviewing experiments.
- Guidelines for categorizing safety of experiments.
- Vetting of investigators and experiments
- External Red-Teaming
- Procedures used by investigators

## Technical

- Firewall, routing, intrusion detection
  and network isolation techniques.
- Neither experimental, nor control network routable Internet.
- Data protection, system protection, and
  state destruction techniques.

# Experiment Safety Panel

- **Experiment description provided by investigator:**
  - Identify containment, isolation, confidentiality, and other security considerations.
- **Panel assesses proposed category:**
  - Determines safety category, level of isolation required
  - Assesses if isolation can be maintained
  - Imposes technical measures to assure isolation requirements are met.

# Experiments: Worms

- **Modeling the scanning characteristics of several worms.**
- **Some common techniques**
  - Use of virtualization extends size of modeled parts of internet.
  - Worms are emulated instead of using live malicious code
- **Live Malicious code**
  - One experiment collected real worm traces on the testbed for use in other experiments.

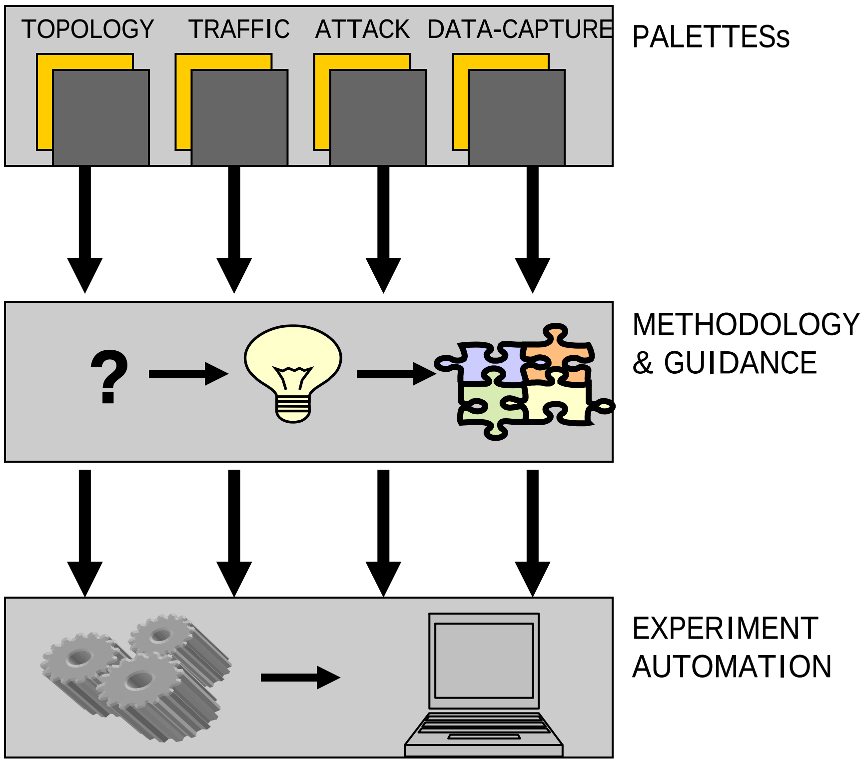
# Experiments: DDoS

- **Tested ability of tools to isolate attack traffic**
  - To pick it out from background traffic
  - Testbed provided environment where it was OK to mount DDoS attack without affecting production links.
- **Tested several real DDoS defense tools**
  - Symantec ManHunt and NFR Sentivist.
- **Resulted in a methodology for analyzing effectiveness of such tools.**

# Experiments: Routing

- **Tested resiliency of secure routing protocols to attack.**
  - Two protocols
    - SBGP, SoBGP
  - Two Attacks
    - Differential Damping Penalty, and Origin AS Changes.
  - Two detection methods:
    - Signature and statistics-based
- **Testbed enabled large scale experiment that could not have been performed on the production network.**

# Improving Usability




## ***Security Experimenters Workbench***

- ***Experimenter's select from a palette*** **of predefined elements: Topology, Background and Attack Traffic, and Packet Capture and Instrumentation**
- ***Our Methodology*** **frames standard, systematic questions that guide an experimenter in selecting and combining the right elements**
- ***Experiment Automation*** **increases repeatability and efficiency by integrating the process to the DETER testbed environment**

# Lessons Learned

- **Security Experiments tend to be Larger**
  - Malicious code is designed to spread network wide, and effects are not seen until significant infection occurs.
- **Support for special hardware**
  - Experimenters need ability to test their own boxes, not just code.
- **Common data collection tools very important**
  - Should not leave this to experimenters. Need ability to compare across experiments.
- **Most experiments do not need strongest containment**
  - Most of our security experiments did not use live malicious code, and vlan and firewall approaches were sufficient for containment.

# Distribution of US DETER users


Source: John Hickey

# For More Information

## For updates and related information

- http://www.isi.edu/deter
- http://www.deterlab.net
- http://www.emulab.net
- http://clifford.neuman.name/publications/2007/200708-usecdw-deter-design-deploy/
- http://clifford.neuman.name/
- http://ccss.usc.edu/

This research was supported by funding from the United States National Science Foundation and the United States Department of Homeland Security under contract numbers ANI-0335298 (DETER) and CNS-0454381 (DECCOR), and by the Department of Homeland Security, and Space and Naval Warfare Systems Center, San Diego, under Contract number N66001-07-C-2001. Opinions, findings, conclusions and recommendations expressed in this paper are those of the authors and do not necessarily reflect the views of the National Science Foundation (NSF), the Department of Homeland Security, or the Space and Naval Warfare Systems Center, San Diego. Juniper Networks and Hewlett-Packard donated equipment used by the DETER testbed. Donations were also received from Sun Microsystems and Dell through their University Discount programs.