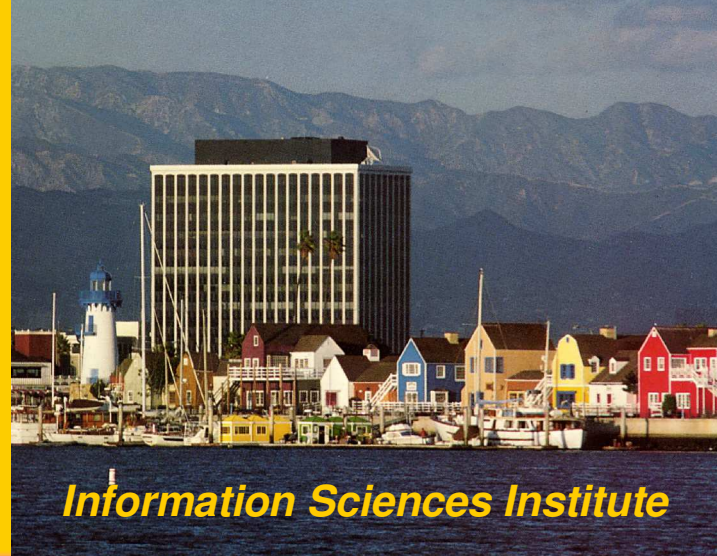


USC Viterbi
School of Engineering

Berkeley
University of California

SPARTA



Information Sciences Institute



Experience with DETER

A Testbed for Security Research

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

Clifford Neuman
Director, USC Center for
Computer Systems Security

March 1, 2006 TridentCom 2006

Barcelona, Spain

WWW.ISI.EDU/DETER

USC

... 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.

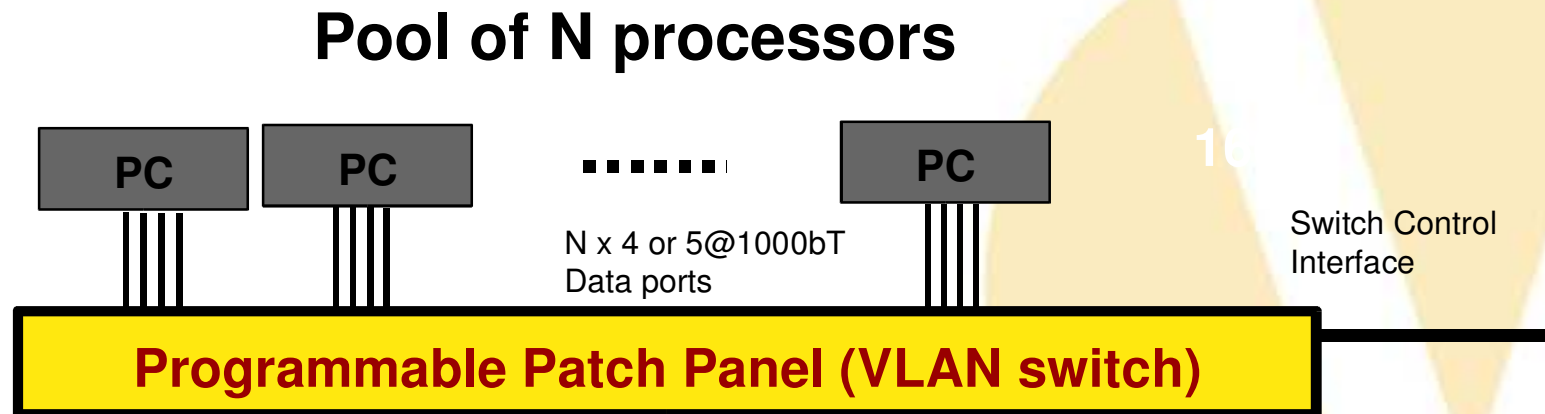
- **Facilitate scientific experimentation**
- **Establish baseline for validation of new approaches**
- **To protect the public internet from the side effects of security experiments**
 - Saturated Links
 - Broken routing
 - Exfiltration of malicious code
- **Provide access for wide community of users**

To Meet These Goals 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

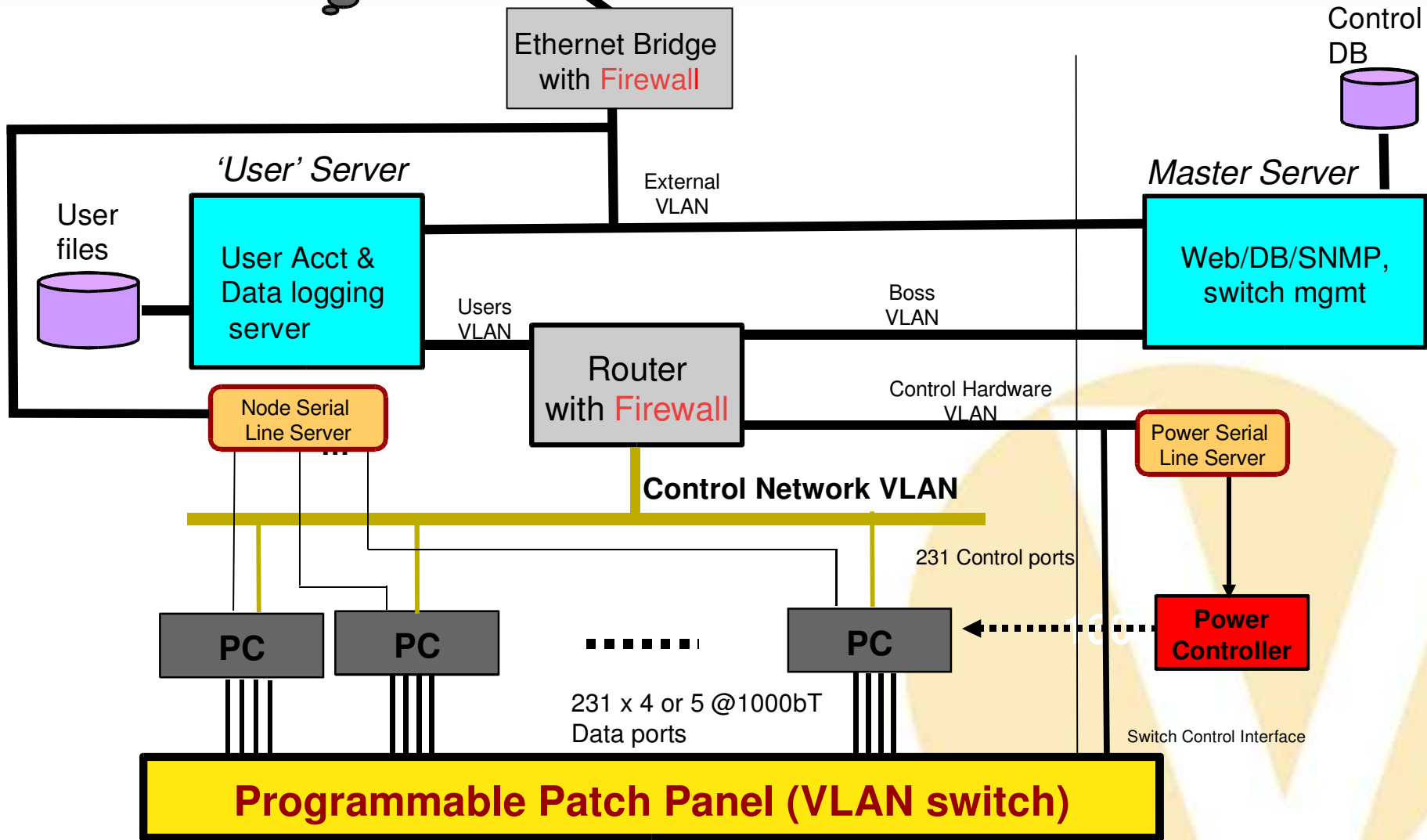
DETER Experimental Network Is Based On Emulab

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



- **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



Two clusters: USC -ISI, UCB

One control site (ISI)

- One user entry point, accounts, control

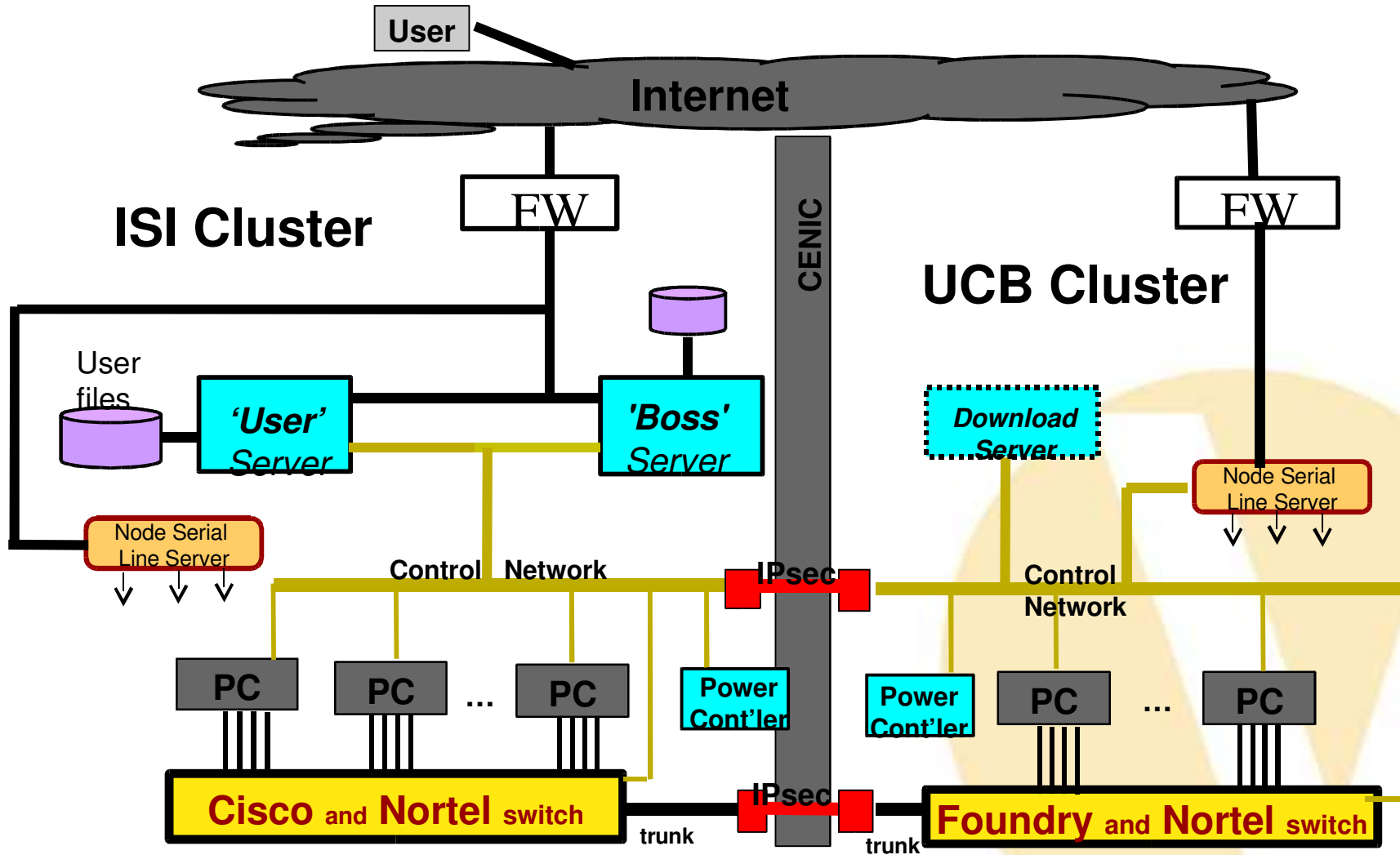
Connection

- CENIC: CaIREN-HPR

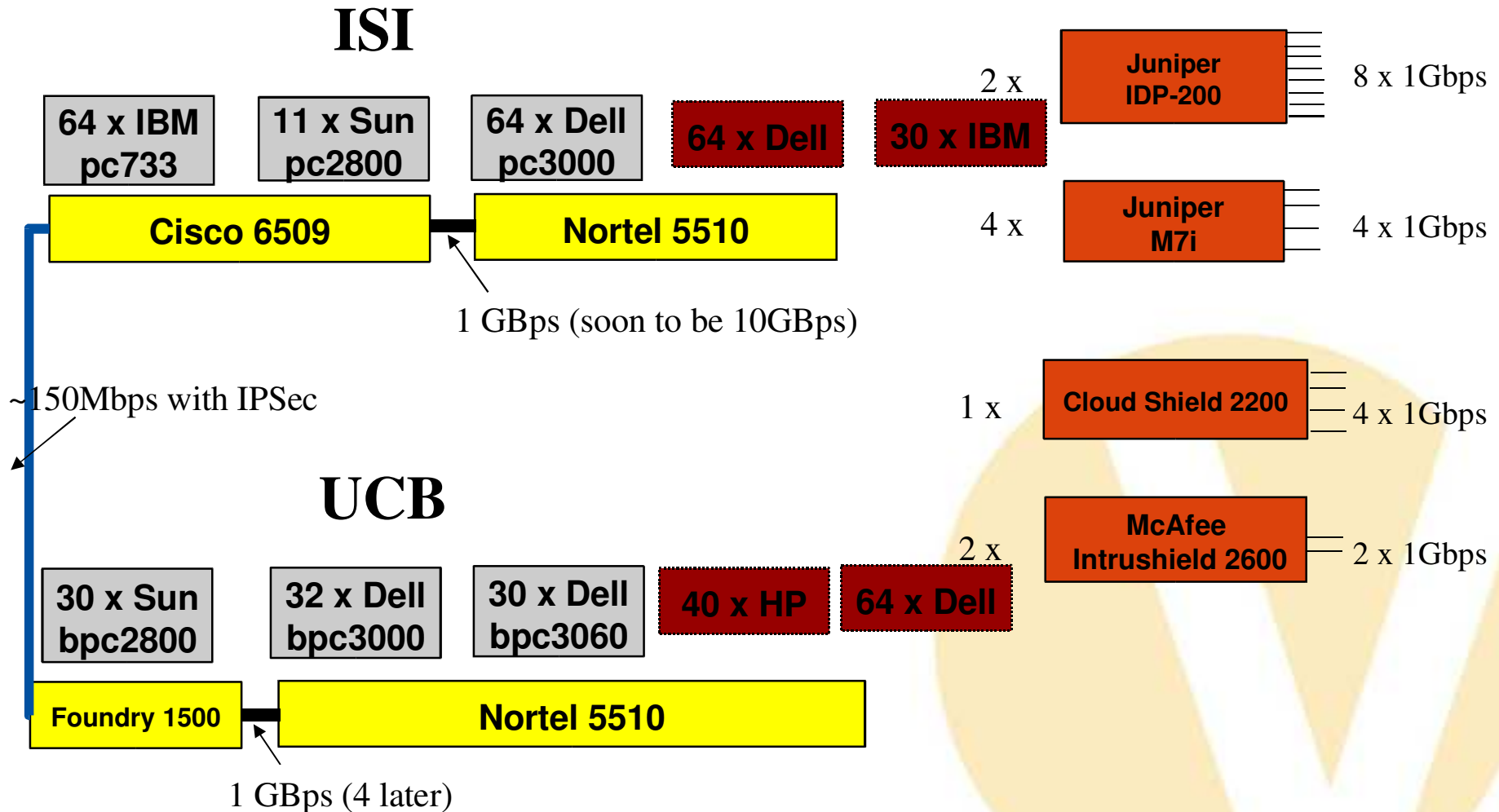
VLAN switches interconnected using proprietary layer 2 tunnels

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

Architectural Diagram



Hardware Status and Plan



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 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.

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

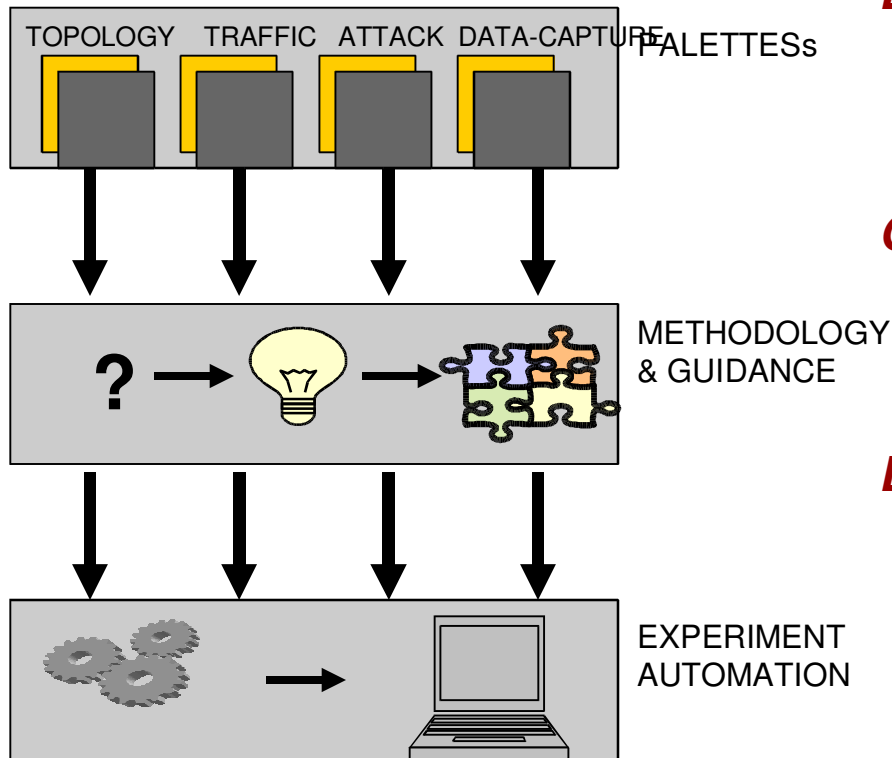
- Firewall, routing, intrusion detection and network isolation techniques.
- Neither experimental, nor control network routable Internet.
- Data protection, system protection, and state destruction techniques.

- **Experiment 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.

- **Modeling the scanning characteristics of several worms.**
 - One example will be discussed in next talk.
- **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 in development to collect real worm traces for use in other experiments.

- **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.**

- **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.**



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

- **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.

Access to Testbed

- Open to community – request via **email: deterinfo@isi.edu**
- Important addresses:
 - **www.isi.edu/deter**
 - **www.isi.deterlab.net**
 - **www.emulab.net**

