Cyber Defense Technology Experimental Research (DETER) and Evaluation Methods for Internet Security Technology (EMIST)

Terry V. Benzel
Information Sciences Institute
University of Southern California

DETER + EMIST: Background

- Inadequate wide scale deployment of security technologies
  - Despite 10+ years investment in network security research
- Lack of experimental infrastructure
  - Testing and validation in small to medium-scale private research labs
  - Missing objective test data, traffic and metrics

DETER+EMIST Vision

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

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

Long Term Objectives

Create reusable library of test technology for conducting realistic, rigorous, reproducible, impartial tests

- For assessing attack impact and defense effectiveness
- Test data, test configurations, analysis software, and experiment automation tools

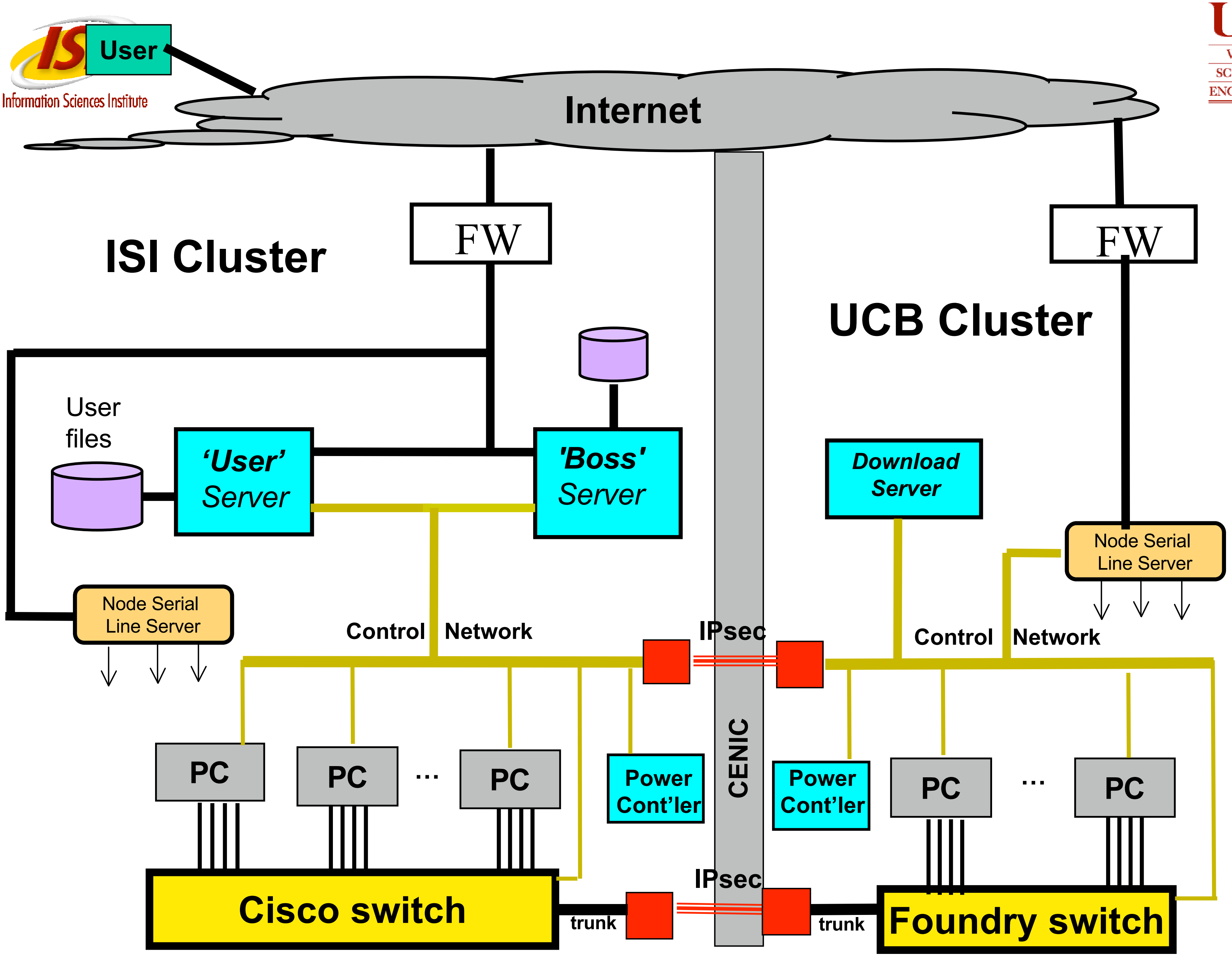
Provide usage examples and methodological guidance

- Recommendations for selecting (or developing) tests and interpreting results
- Test cases and results, possibly including benchmarks

Facilitate testing of prototypes during development and commercial products during evaluation

DETER Architectural Plan

- Construct homogeneous emulation clusters based upon University of Utah’s Emulab
- Implement network services – DNS, BGP
- Add containment, security, and usability features to the software
- Add (controlled) hardware heterogeneity
- Evaluate usefulness of other testbed approaches – esp. overlays like Planetlab



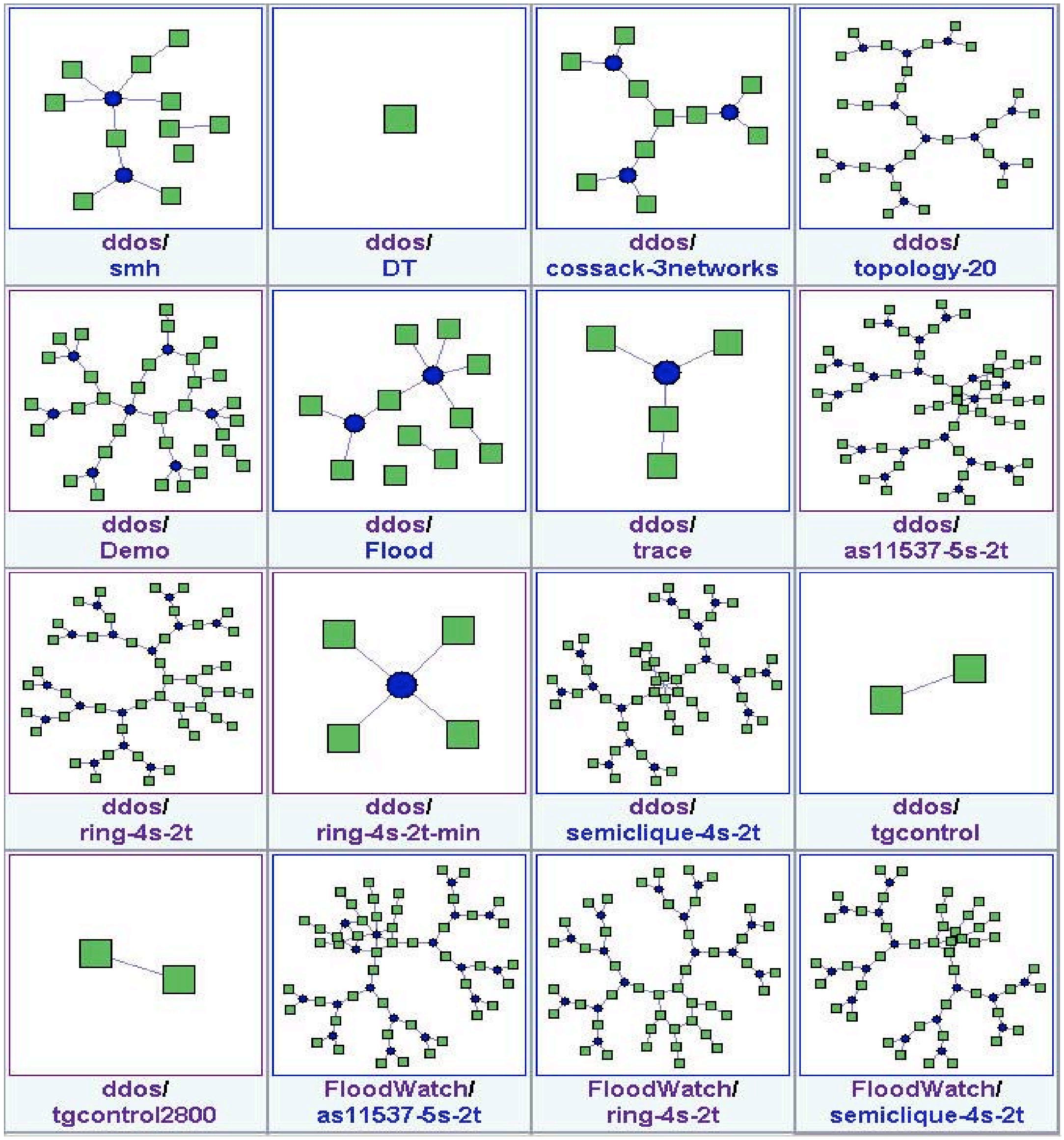
USC VITERBI SCHOOL OF ENGINEERING

8/9/05

DETER Testbed Infrastructure

- 201 (139 + 62) PC nodes in 4 types
- 9 control plane PC’s
- 9 switches for control, experimental, and administrative purposes
- Serial expanders for 201 nodes
- Remote power controllers
- IPSec tunnel between ISI and U.C. Berkeley

Example DETER Topologies



Experimenters Workshop September 28, 2005

- Second workshop
  - Demonstrations of 6 – 8 current experiments
  - Working groups on experiments
    - DDOS
    - Worms
    - Routers
- For information on workshops or testbed use
- Email: deterinfo@isi.edu

Access to Testbed

- Open to community – request via email: deterinfo@isi.edu
- Important addresses:
  - www.isi.edu/deter
  - www.isi.deterlab.net
  - http://emist.ist.psu.edu
  - www.emulab.net
- Hiring – email tbenzel@isi.edu