



The **DETER** Project

The DETER Project: Leading-edge Experimental Facilities and Methodologies for the Cyber-Security Research Community

Terry Benzel
Deputy Director, Cyber Networks Division
USC Information Sciences Institution
tbenzel@isi.edu
310-448-9438



The DETER Project

- A research program:
 - To advance the tools and methodologies for experimental cybersecurity research
- A testbed facility:
 - To serve as a publicly available national resource...
 - ...supporting a broad base of users and experiments
 - ... and act as a technology transfer and evangelization vehicle for our and others' research in experimental methodology
- A community building activity:
 - To foster and support collaborative science...
 - ...effective and efficient leverage and sharing of knowledge



Research Goals

- Advance our understanding of experimental cybersecurity *science and methodologies*
 - Enable new levels of rigor and repeatability
 - Transform low level results to high level understanding
 - Broaden the domains of applicability
- Advance the *technology of experimental infrastructure*
 - Develop technologies with new levels of function, applicability, and scale
- Provide operational facility as national resource
 - Open for anyone to use
 - Easy application process
- Share knowledge, results, and operational capability
 - Facility, data and tools
 - Community and knowledge



The DETER Facility

A general purpose, flexible platform for modeling, emulation, and controlled study of large, complex networked systems

- Elements located at USC/ISI (Los Angeles), UC Berkeley, and USC/ISI (Arlington, VA)
- Funded by NSF and DHS, started in 2003
- Based on Emulab software, with focus on security experimentation
- Shared resource – multiple simultaneous experiments subject to resource constraints
- Open to academic, industrial, govt researchers essentially worldwide – very lightweight approval process



Physical Platform



- ~550 PC-based nodes
 - Berkeley, CA - ~200 Nodes
 - Los Angeles, CA - 330 Nodes
 - Arlington, VA – 20 Nodes
- Interconnect (2010)
 - 1 Gb/s – LA-UCB
 - 1-10 Gb/s LA-Arlington
- Local and Remote access



Advanced Infrastructure Capabilities

- Efficiency and scalability
 - Advanced virtualization strategies
 - Platform support for data-intensive scenarios"
- High-performance co-processing
 - NetFPGA-based node deployment
 - Dedicated hardware modules, e.g. packet monitors





Key Capabilities

- Technical elements
 - DETER Core
 - Scalable Modeling and Emulation
 - Federation
 - Risky Experiment Management
 - Multiparty Experiments
 - Experiment Lifecycle Management

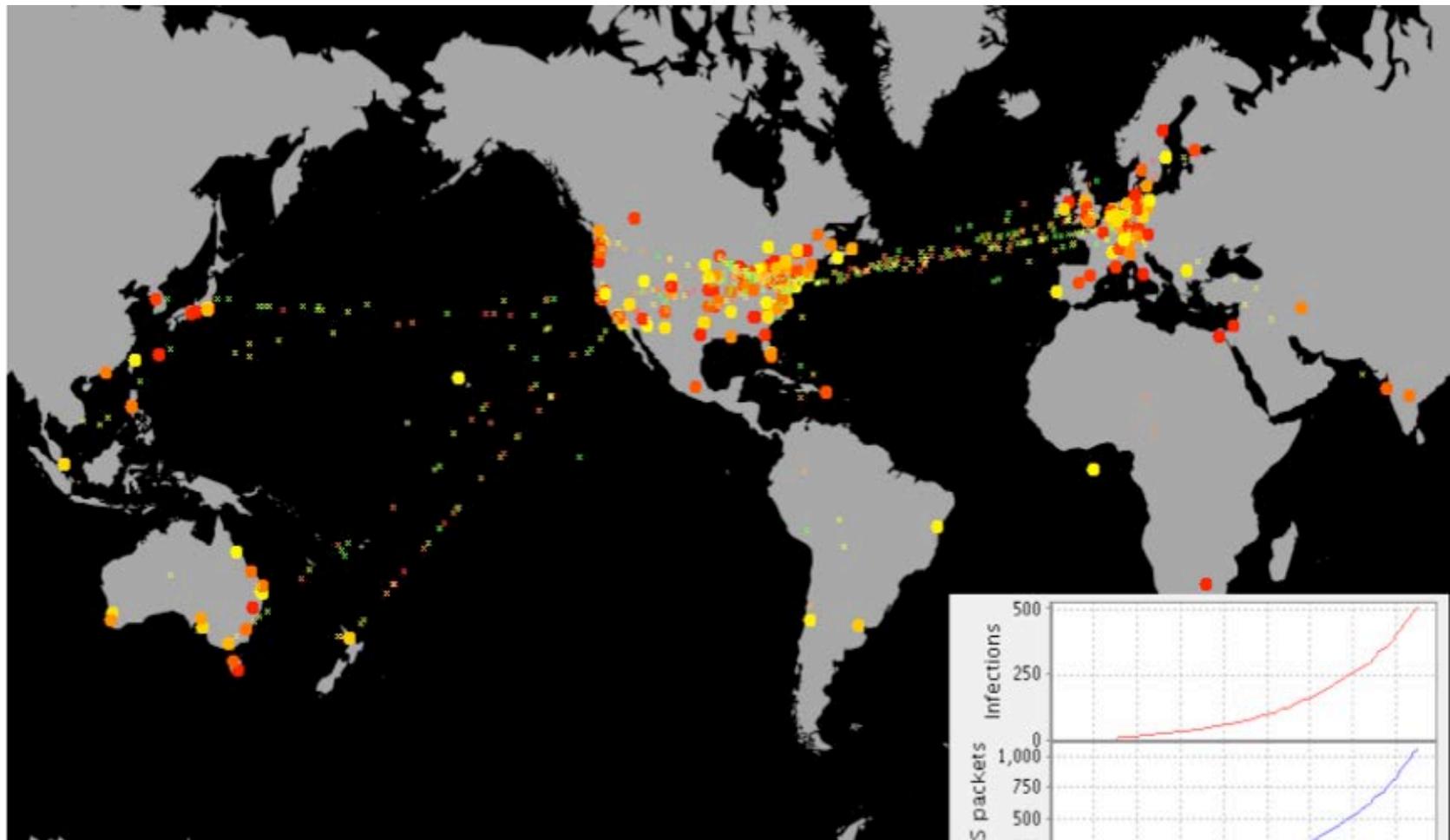


Scalable Modeling and Emulation

- The problem:
 - Traditional testbeds can model and emulate *small* systems at a *fixed* level of fidelity.
- The challenge:
 - Many real problems require modeling of *large, complex* systems at an *appropriate* (“good enough”) level of fidelity.
 - That level may be *different* for different parts of the modeled system.
 - Think of this as “smearing the computation power around to just where it’s needed”.



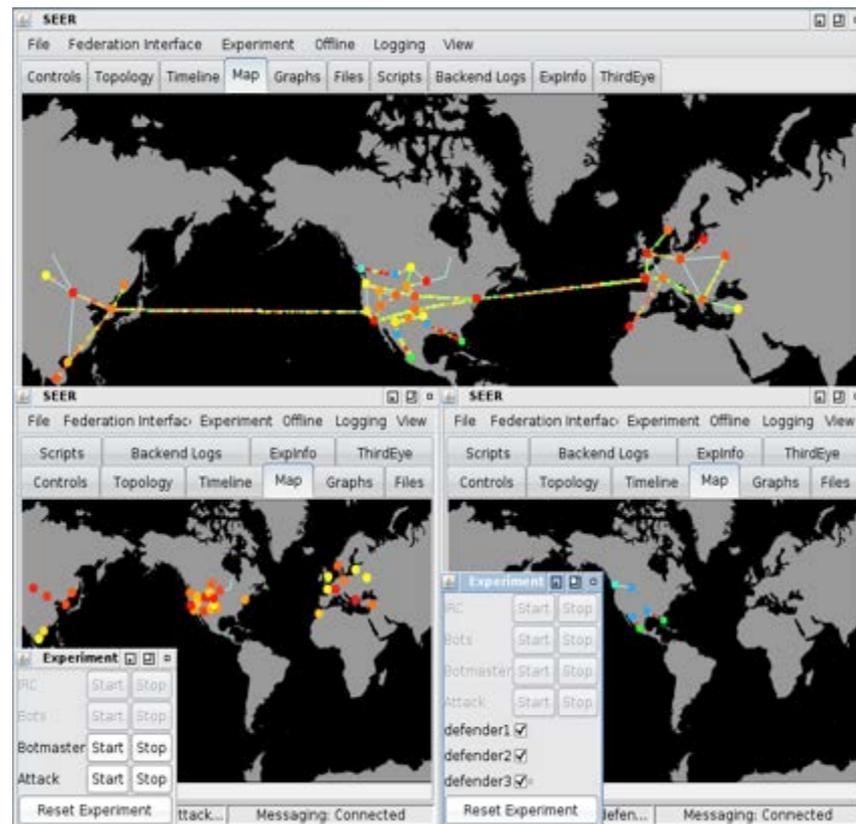
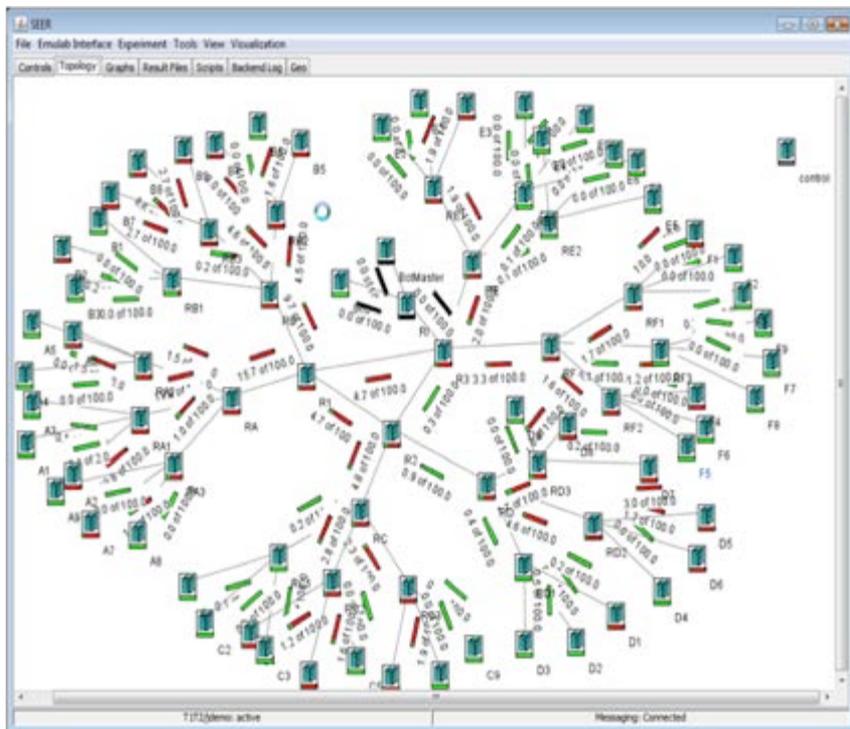
100 K-Node Worm/Botnet/DDOS Scenario



The **DETER** Project



Control, Analysis, and Visualization Interfaces and Tools



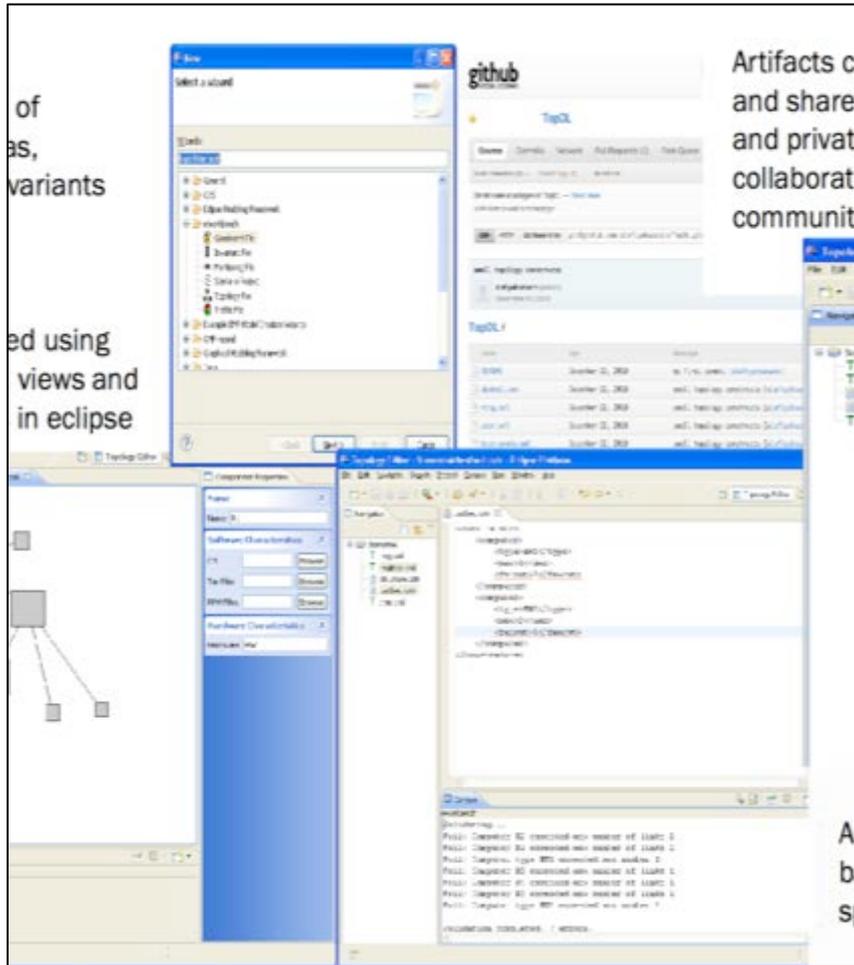


Scenario Lifecycle Management

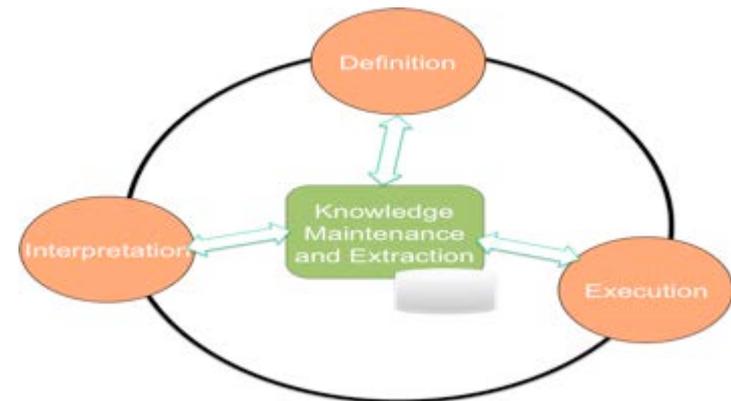
- Most testbed tools focus on *creating* and *running* an experiment. Much less attention is paid to other important steps in the process
- Develop a model for workflow over the full lifecycle of an experiment, and capture that model in methodologies and tools



Scenario Lifecycle Management



- Key Observation: isomorphism to software engineering lifecycle
- Strategic Approach: leverage techniques and lessons learned from modern software development methodologies and tools
- Implementation Approach: Leverage Eclipse



USING DETER



Using DETER

- All you need is a Web browser and an SSH client
- Open a user account (open to all users)
- Log on to our Web site – <https://isi.deterlab.net>
- Run experiments
 - Create a topology, or retrieve an existing one
 - Nodes are assigned to you
 - Load software you need or use DETER sw to create traffic and events of interest, deploy defenses, monitor (SSH)
- Swap out (return nodes) or terminate (if no longer needed) experiments



Using DETER – Open account, manage experiments

161 detelab.net - DeterLab: Cyber-Security Experimentation and Testing Facility



Current Experiments

42	Active
3	Idle
4136	Swapped
63	Free PCs

Information

DeterLab
[DeterLab Documentation](#)
[DeterLab Support](#)
[Education with DeterLab](#)
[Projects using DETERlab](#)
[DETER Project](#)
[News \(October 3\) NEW!](#)

or

Vers: 4.296 Build: 06/22/2012 Sun Oct 07 9:30pm PDT

DeterLab: Cyber-Security Experimentation and Testing Facility

Regularly Scheduled downtime: Wednesdays: 5PM-7PM, Saturdays: 10AM-1PM Pacific Time.

Welcome to DeterLab -- the shared facility for scientists engaged in research, discovery, development, experimentation, and testing of new cyber-security technology. DeterLab is operated by the [DETER Project](#) team, whose research results and lab infrastructure innovations -- used by DeterLab's worldwide research community -- advance the scale, pace, and power of security technology development. Over [200 organizations](#) are using DeterLab for cyber-security experimentation and education.

Registered users can [login](#) for remote access to their DeterLab workbench, a Web-based interface that DeterLab experimenters use to develop, configure, operate, and observe their experiments.

To become a new user of DeterLab, first [register](#) to create a new DeterLab project, or [join](#) an existing project -- or [contact us](#) to learn more about getting started with DeterLab. More information on DeterLab is available on the [public DeterLab web site](#), and via the following links:

- [Support](#) for DeterLab experimenters
- [Documentation](#) of DeterLab facilities and tools
- [Overview of Supported Software](#), the operating systems available to experimenters
- [Overview of Installed Hardware](#) available for experimenters to use
- [SEER](#) toolkit for DeterLab experimenters
- [FEDD](#), the framework for federation between DeterLab and other testbeds
- [Containers](#), the infrastructure for creating large scale experiments through virtualization.
- [ABAC](#), the facility for Attribute Based Access Control
- [DeterLab Tools](#), a guide to several tools for experiment development, operation, and control.



[DETER Project](#) | [PRIVACY POLICY](#) | [CONTACT](#)

Copyright © 2000-2012 USC Information Sciences Institute and University of Utah





Using DETER – Bind an experiment to the facility

97 Free PCs, 0 reloading				
pc2133	0	bpc2800	0	
bpc2133	4	bpc3000	17	
pc3000	tunnel	0	pc3060	11
pc3100	4	bpc3060	29	
bpc1400	0	bpc800	0	
bvx2200	8	bpc2133m	0	
pc2300	1			

- **If you have an NS file:**
You may want to [syntax check it first](#)
- **If you do not have an NS file:**
[New GUI editor](#) - An enhanced Java applet for editing topologies.
The older [NetBuild GUI](#) can be used to graphically create topologies. ([Additional information](#)).
Or, you can download the Emulab [client](#) and graphically create one from your desktop.



Select Project:	<input type="text" value="Please Select"/>
Group:	<input type="text" value="Default Group"/> (Must be default or correspond to selected project)
Name: (No blanks)	<input type="text"/>
Description: (A concise sentence)	<input type="text"/>
Your NS file: <input type="button" value="Syntax Check"/>	Upload (500k max) <input type="text"/> <input type="button" value="Browse..."/> or On Server (/proj, /users, /groups) <input type="text"/>
Swapping:	<input checked="" type="checkbox"/> Idle-Swap: Swap out this experiment after <input type="text" value="4"/> hours idle. If not, why not? <input type="text"/> <input type="checkbox"/> Max. Duration: Swap out after <input type="text" value="16"/> hours, even if not idle.
Linktest Option:	<input type="text" value="Skip Linktest"/> <input type="button" value="(What is this?)"/>
<input type="checkbox"/> Batch Mode Experiment (See Tutorial for more information)	
<input type="checkbox"/> Do Not Swap In	
<input type="button" value="Submit"/>	

Handy Links:

- View a [list of OSIDs](#) that are available for you to use in your NS file.
- Create your own [custom disk images](#).



Using DETER – Manage an experiment

isi.deterlab.net – Experiment (Share/grassroots)

deterlab.net https://www.isi.deterlab.net/showexp.php3?pid=Share&eid=grassroots

Most Visited Getting Started Google Calendar Latest Headlines Apple Amazon eBay Yahoo! News

isi.deterlab.net – Experiment (Shar... +

deterlab
based on emulab

My DETERlab | Logout | News | Contact Us | Search Documentation Go

Information Experimentation

Experiment (Share/grassroots)

Settings Visualization NS File Details

Experiment Options

- [View Activity Logfile](#)
- [Cancel Experiment Swapin](#)
- [Terminate Experiment](#)
- [Modify Settings](#)
- [Run LinkTest](#)
- [Show History](#)
- [Duplicate Experiment](#)

94 Free PCs, 0 reloading												
pc2133 0	bpc2800 0	bpc2133 1	bpc3000 17	pc3000 23	pc3000 11	pc3100 4	bpc3060 29	bpc1400 0	bpc800 0	bvx2200 8	bpc2133m 0	pc2300 1

Name:	grassroots
Description:	demo of deter for grassroots
Project:	Share
Group:	Share
Experiment Head:	sunshine
Created:	2010-02-22 12:29:50
Last Swap/Modify:	2010-02-22 12:30:06 (sunshine)
Idle-Swap:	Yes (after 4 hours)
Max. Duration:	Yes (after 16 hours)
Save State:	No
Path:	/proj/Share/exp/grassroots
Status:	active
Linktest Level:	0
Min/Max Nodes:	8/8 (estimates)
Virtual Nodes:	Unknown
Mem Usage Est:	0
CPU Usage Est:	3
Locked Down:	No (Toggle)
Sync Server:	attacker1
Index:	14314

[The Deter Project] [Information Sciences Institute] [and University of California at Berkeley]
[Flux Research Group] [School of Computing] [University of Utah]
Copyright © 2000-2010 The University of Utah and Information Sciences Institute

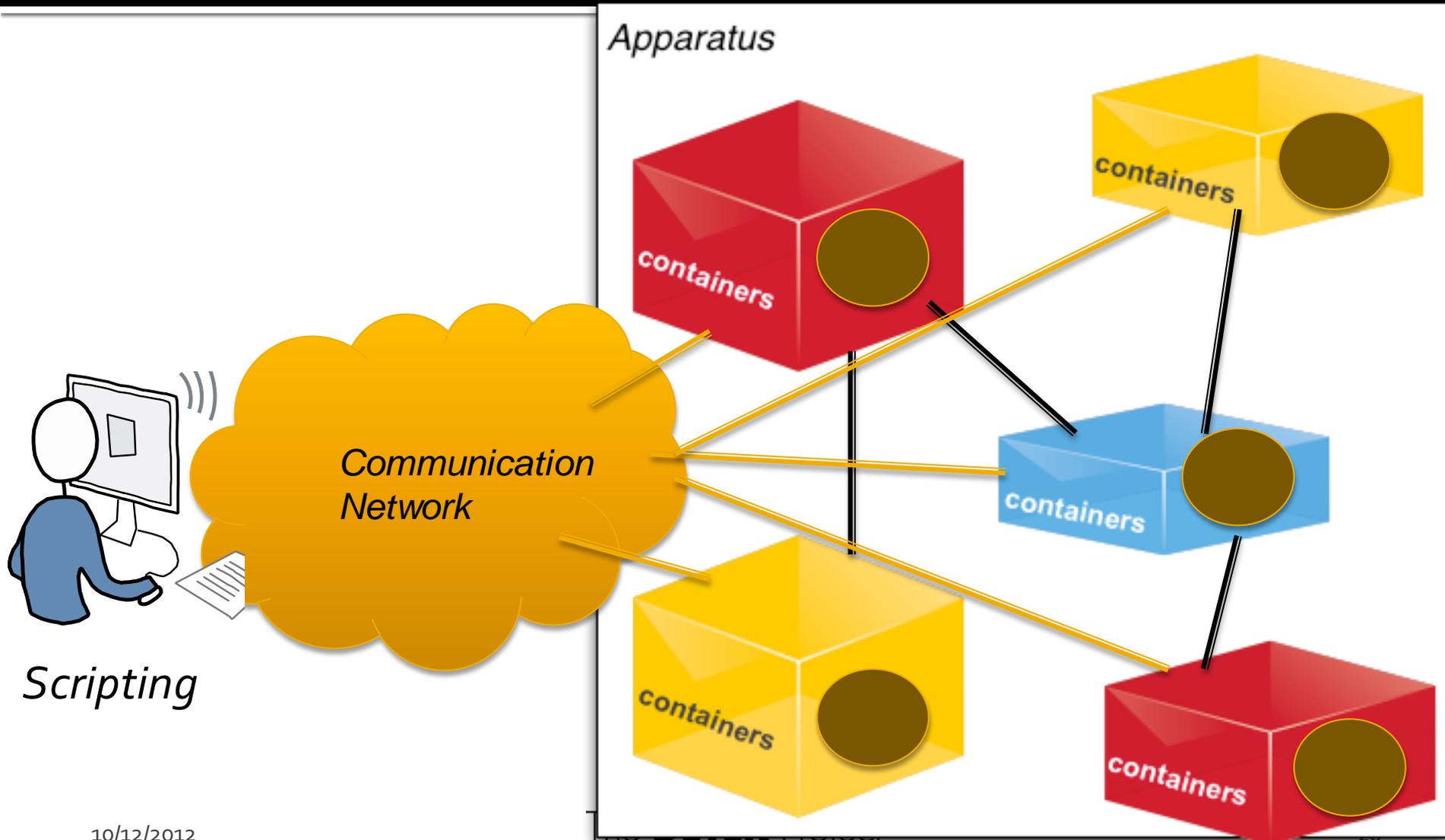


New Methodologies and Tools

- Containers: Abstraction-Guided Experiment Realization
 - Multi-axis resource use
 - Virtualization
 - Simulation
 - Programmable Hardware
- *Montage AGent Infrastructure (MAGI)*
 - Second generation control technology
 - Enable large scale
 - Support complex control



MAGI Frame of Reference





Community and Outreach

- Content sharing support
 - Experiments, data, models, recipes
 - Class materials, recent research results, ideas
- Shared spaces
 - Outreach: Conferences, tutorials, presentations
 - Share and connect: Website, exchange server
 - Common experiment description: Templates
 - Build community knowledge: domain-specific communities
- Education support
 - NSF CCLI grant: develop hands-on exercises for classes
 - Moodle server for classes on DETER



DETER User Institutions

Government

Air Force Research Laboratory

DARPA

Lawrence Berkeley National Lab

Naval Postgraduate School

Sandia National Laboratories

Industry

Agnik, LLC

Aerospace Corporation

Backbone Security

BAE Systems, Inc.

BBN

Bell Labs

Cs3 Inc.

Distributed Infinity Inc.

EADS Innovation Works

FreeBSD Foundation

iCAST

Institute for Information Industry

Intel Research Berkeley

IntruGuard Devices, Inc.

Purple Streak

Secure64 Software Corp

Skaion Corporation

SPARTA

SRI International

Telcordia Technologies

Academia

Carnegie Mellon University

Columbia University

Cornell University

Dalhousie University

DePaul University

George Mason University

Georgia State University

Hokuriku Research Center

ICSI

IIT Delhi

IRTT

ISI

Johns Hopkins University

Lehigh University

MIT

New Jersey Institute of Technology

Norfolk State University

Pennsylvania State University

Purdue University

Rutgers University

Sao Paulo State University

Southern Illinois University

TU Berlin

TU Darmstadt

Texas A&M University

UC Berkeley

UC Davis

UC Irvine

UC Santa Cruz

UCLA

UCSD

UIUC

UNC Chapel Hill

UNC Charlotte

Universidad Michoacana de San Nicolas

Universita di Pisa

University of Advancing Technology

University of Illinois, Urbana-Champaign

University of Maryland

University of Massachusetts

University of Oregon

University of Southern California

University of Washington

University of Wisconsin - Madison

USC

UT Arlington

UT Austin

UT Dallas

Washington State University

Washington University in St. Louis

Western Michigan University

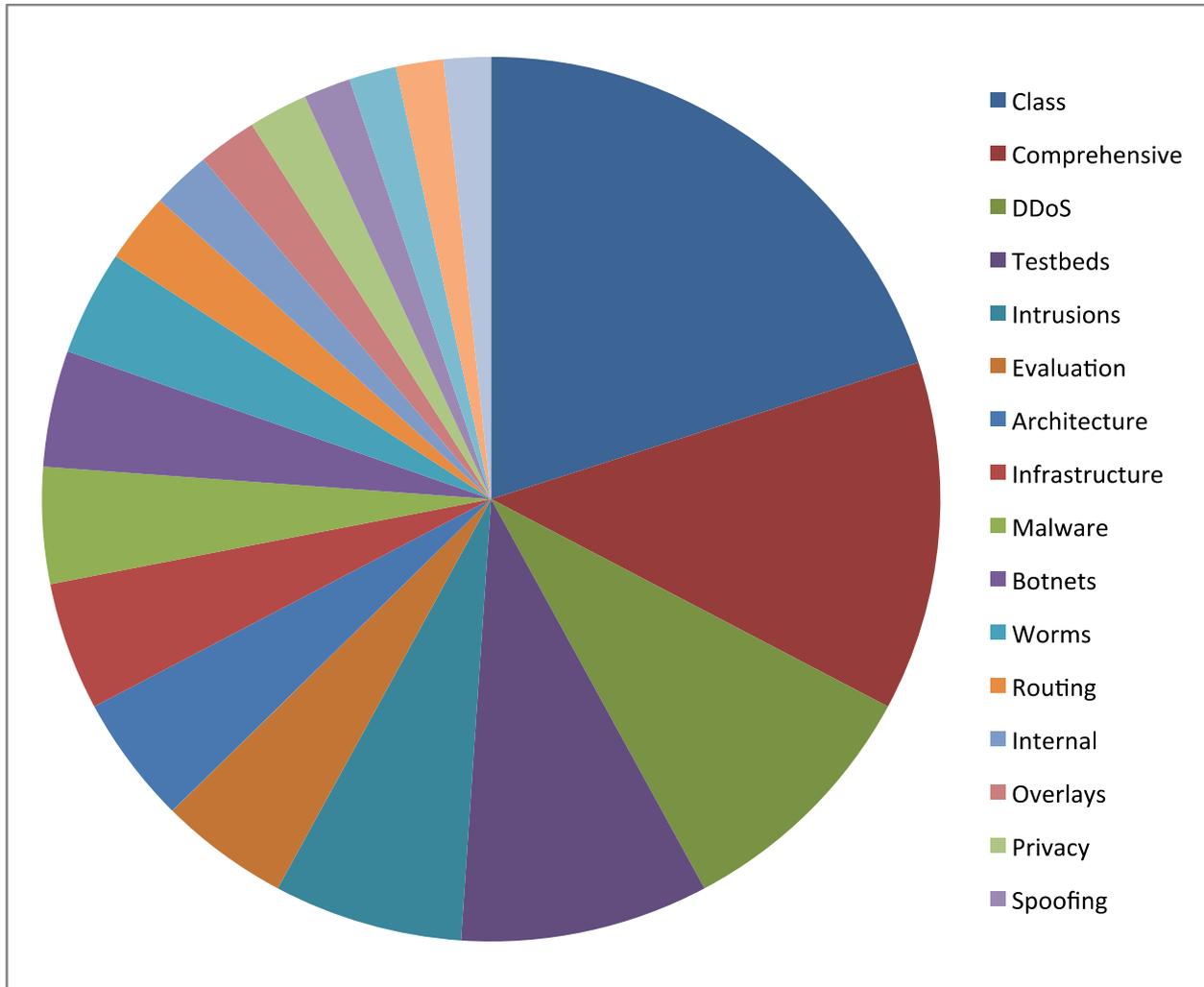
Xiangnan University

Youngstown State University

The **DETER** Project



DETER User Research





Conclusion

- **Benefits**
- Transformative research and facility for cyber security R&D
- Experimental science:
 - Fostering fundamental understanding world complexity
- Contribution transformation of field
- Proactive robustness and away from reactive security
- **Join DETER – deter-project.org**
- Growing DETER Community increasingly engaged in experimental science of cyber security
- Collaboration key part of DETER mission