Terry Benzel
USC Information Sciences Institute
May 19, 2013

The Science of Cyber Security Experimentation
Cyber-threat continues to accelerate
Far fewer cyber-defense technologies
Gap between threat and defense widened
Increasingly sophisticated attack technology
  unprecedented power
  resources
  global reach
Increasingly by nation states
What Can We do About It?

Solution – build less vulnerable systems to begin with!

Create fundamental understanding and reason about systems through experimental means

Key aspect – enable science based experimentation

Hard Problem
1. Have an idea for a “new” tool that would “help” security

2. Program/assemble the tool (the majority of the work)

3. Put it on your local net

4. Attack your system

5. Show the tool repels the attack

6. Write up “the results” and open-source the tool

7. (optional) Start up a company which might succeed
Instead - Objectives

Perform experimental research of scale and complexity representative of the real world

Extract understanding through experimental research

Collect, leverage, and share experimental artifacts and learnings
Cyber Security Experimentation

Class of experimental cyber science applied to sets of problems - networked cyber systems and often cyber physical networked systems

Goal - enable experimental cyber science aimed at study of behavior, phenomena, providing fundamental understanding
The DETER Project
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
DETERLab = Hardware + Software

Hardware
  Experiment nodes, Ethernet switches
  https://trac.deterlab.net/wiki/Installation

Open Source Software
  DETER manages stable repository
  Communities can copy/ specialize this repo
  Communities can share, exchange
  DETER accepts contributions to stable base
Physical Platform

- ~440 PC-based nodes
  - Berkeley, CA - ~200 Nodes
  - Los Angeles, CA - 220 Nodes
  - Arlington, VA – 20 Nodes

- Interconnect
  - 1 Gb/s - LA-UCB
  - 1-10 Gb/s LA-Arlington

- Local and Remote access
Key Capabilities

Technical elements
  DETER Core
  Scalable Modeling and Emulation
  Risky Experiment Management
  Multiparty Experiments
  Federation
  Partner Cluster Deployment
RESEARCH PROGRAM
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

Share knowledge, results, and operational capability
   Facility, data and tools
   Community and knowledge
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”.
Containers

DETER **containers** use virtualization to support larger experiments.

Containers use several different types of virtualization.

Selecting different virtualization types allows a trade-off:
- One container per physical machine → high fidelity.
- More containers per physical machines → less fidelity.
Defining Experiment Scenarios

Experiment Topology
Different Scenarios: Different Abstractions

BGP Security

Worm Propagation
Methodologies, Models and Technologies

Representing the (near infinite) world in the (rather finite) testbed

Automating everything that can be automated for repeatable, realistic testing

Automating (albeit imperfectly) that which can’t be automated (e.g. Humans)
Experiment scenarios require many disparate elements to be combined within a single overall scenario. These elements must be:
- deployed, initialized, configured,
- monitored and coordinated
- instrumented with real-time and post-mortem data collection
...throughout the execution of the experiment.

DETER’s MAGI agent infrastructure provides an architecture for scalable control and instrumentation.
Experiment Control & Monitoring

Scalable and flexible
Rich Control Semantics
Montage Agent Infrastructure

Leverage strengths of previous generation technologies
  tevc, SEER

Control Semantics
  time based and event based
  triggers
  workflows

25+ agents and growing
traffic, monitoring

Users and contributors
  DeterLab Users
  Education
DETERLab
Federation
Multiple Communities

Specialized environments
Different domains of expertise
Partner Clusters

DeterLab cluster at the partner’s facilities
  Partner’s hardware and network resources

Federation technology enables interoperation with DeterLab
Current partners underway
  Pacific Northwest National Labs (PNNL)
  University of Illinois, Urbana – Champaign (UIUC)
  Defense Research Department Canada (DRDC)
  BBN Technologies, a Raytheon Company
  Battelle Labs
  SRI International

Different types of organizations and cluster hardware Contributions back to ISI DETER Core
Dynamic Federation

On-demand creation of experimental scenarios spanning *multiple, independently controlled* facilities

Goals and Benefits
- Scale
- Access to unique resources
- Accommodation of usage policy constraints
- Data & knowledge sharing
- Information hiding
DETER-Enabled Federated Testbeds

The Department of Homeland Security (DHS) Science & Technology Directorate Cyber Security Division

The Department of Energy (DoE) Office of Electricity Delivery and Energy Reliability
DEFT Consortium Goals

- Support experimental research
  - Cyber physical systems
  - Wide range of security, reliability, performance, and other challenges

- Provide research infrastructure
- Integrate geographically distributed cyber and physical resources and tools
- Shared, distributed, and federated capability
The DETER Community
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
**Government**
- Air Force Research Laboratory
- DARPA
- Lawrence Berkeley National Lab
- Naval Postgraduate School
- Sandia National Laboratories

**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

**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
Education

Hands on exercises
Students gain from direct observation of attacks and interaction
Pre packaged for both student and teacher
  Buffer overflows, command-injection, middle-in-the-middle, worm
  modeling, botnets, and DoS

Facility support for class administration
Conclusion
Benefits

Transformative research and facility for cyber security R&D

Experimental science:
  Fostering fundamental understanding of world complexity

Contribution transformation of field
Proactive robustness and away from reactive security
Growing DETER Community increasingly engaged in experimental science of cyber security

Collaboration key part of DETER mission

We are HIRING!
    Marina del Rey and Arlington, VA

Join us
http://deter-project.org/