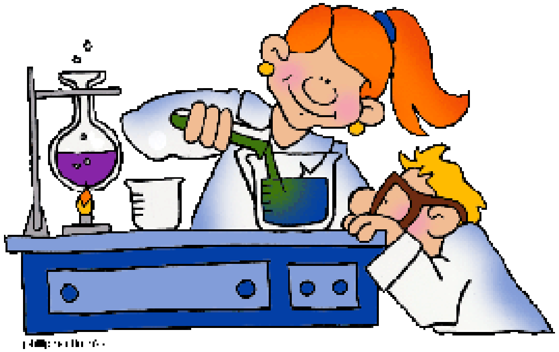
Terry Benzel and Jelena Mirkovic
Information Sciences Institute
University of Southern California

DREAMS:
The DETER Testbed and Beyond

NSF #1842703

Leveling the Playing Field

- The entire world is a testbed for the adversary
  - Endless time
  - Largely undetected
- Researchers with innovative new ideas
  - Need experimental environments
  - To validate defenses they must launch attacks, which are unsafe to launch in the real Internet



- Realistic environments
- Metrics
- Reproducible, reusable experiments
- Validation
- Research to education pipeline

The DETER Project Goals

- Framework for experimental research
  - Scale and complexity representative of the real world
  - Safe experimentation
  - Cybersecurity-specific experimentation tools
- Advance experimentation methodology
  - Experiment validation, artifact understanding
  - Reproducible, reusable experiments, artifact sharing
- Improve cybersecurity education
  - Shared learning platform, innovative and public materials
- Build experimenter communities
  - Workshops and direct outreach

The DETER Project

Research on experimentation and testbeds

DeterLab facility
https://www.deterlab.net

Community and education

Funded by US Department of Homeland Security, NSF, DARPA, DoD

Research

- Multi-resolution virtualization
- Scalable experiment orchestration
- Realistic traffic generation
- Safe live-malware experimentation
- Human behavior modeling in experiments
- Data collection, visualization and situational awareness
- Reproducible, reusable research
- Domain-specific tools and models
- Testbed federation

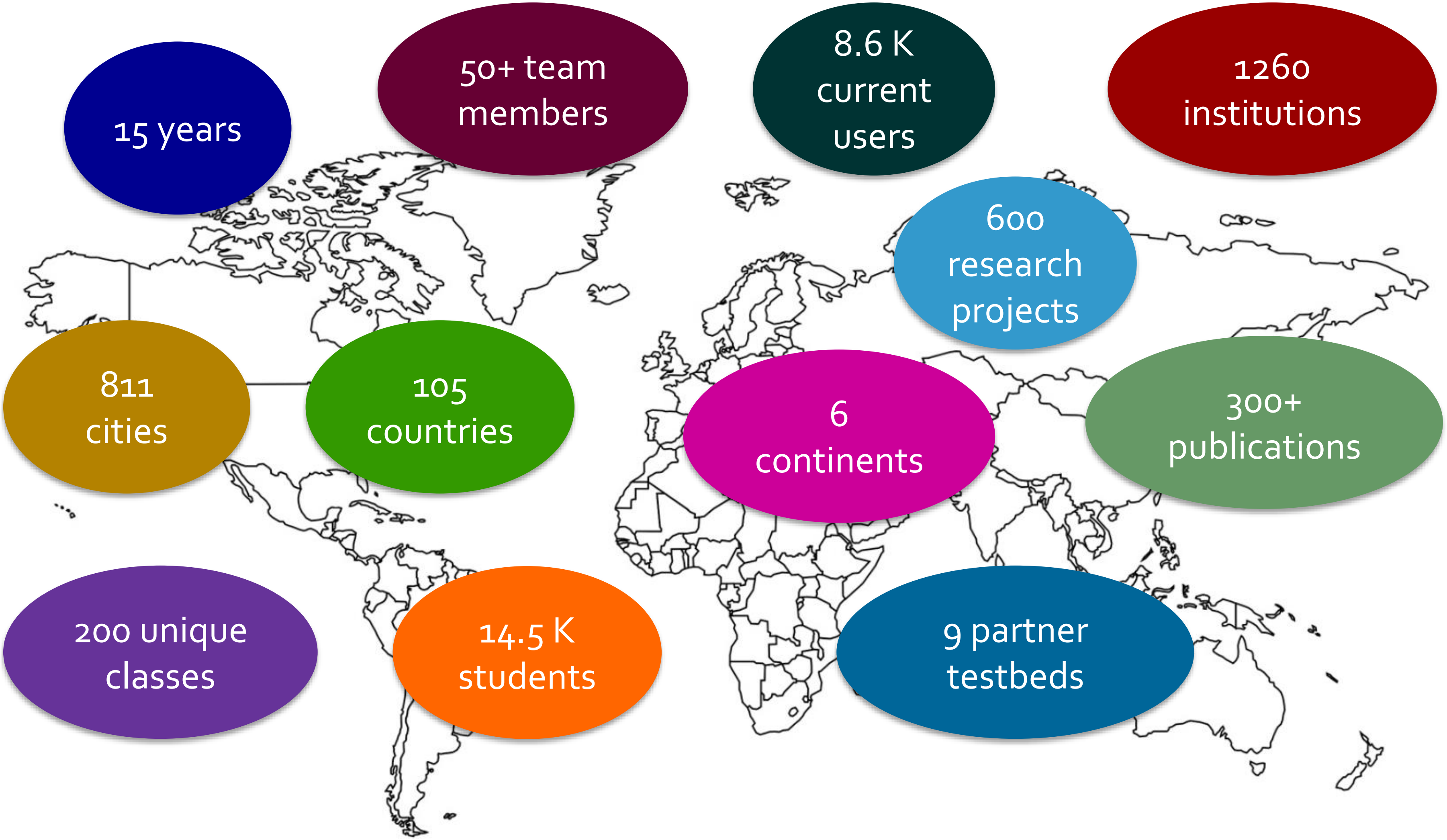
DeterLab Facility

- Remotely-accessible network testbed
  - 700+ nodes at USC/ISI, USC and UC Berkeley,
  - Based on Emulab software, with focus on security experimentation
  - Researchers get exclusive, root access to physical machines connected into custom topologies
- Shared resource
  - Multiple simultaneous experiments
- Public resource
  - Open to academic, industrial, govt researchers worldwide
  - Lightweight approval process

Community and Education

- CSET workshop with USENIX Security
  - 12 years and going strong
- GREPSEC workshop at Oakland S&P
  - Engage minority and women in security, 4 workshops
- CEF – study, workshops, comm. engagement meet.
  - 150+ people from 50+ organizations
- Specialized communities
  - CPS, government, international
- Public materials for cybersecurity education
  - Used in hundreds of classes worldwide

DETER Project In Numbers



15 years

50+ team members

8.6 K current users

1260 institutions

600 research projects

811 cities

105 countries

6 continents

300+ publications

200 unique classes

14.5 K students

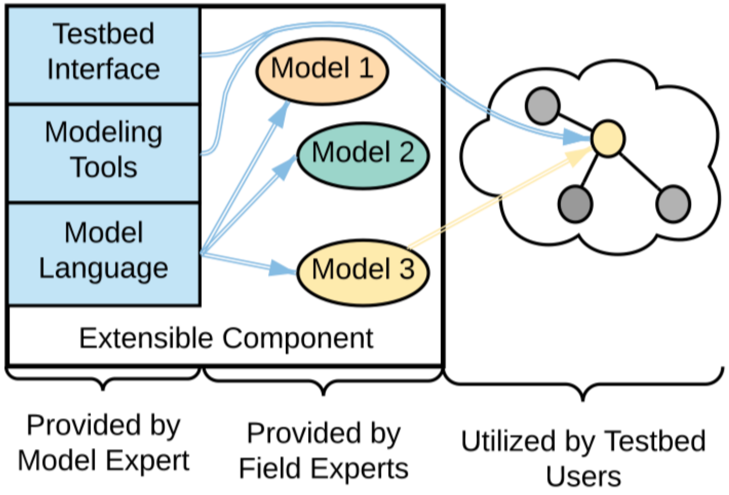
9 partner testbeds

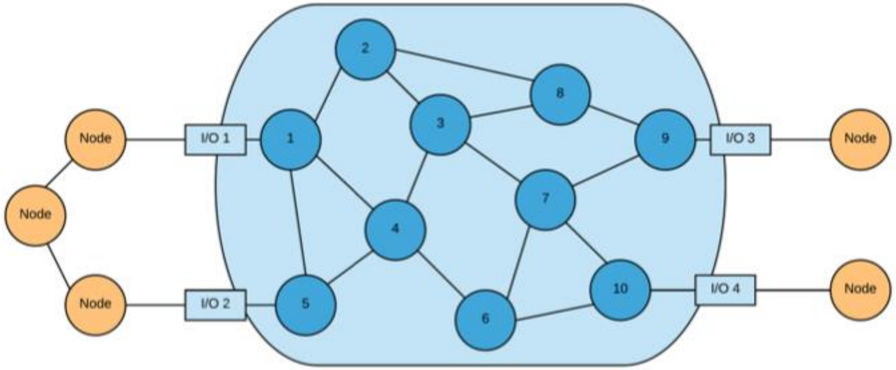
DREAMS Project

- Research – new capabilities
  - Domain-specific components
  - Binary analysis
  - Modeling human factor in experiments
- Education – new and improved features
  - New materials
  - Customized materials to prevent cheating
  - Dockerization to reduce resource demand
- Operations – improve robustness and usability
  - Improve error detection and diagnosis
  - Security analysis of DeterLab code
  - Resource reservations

Extensible Components

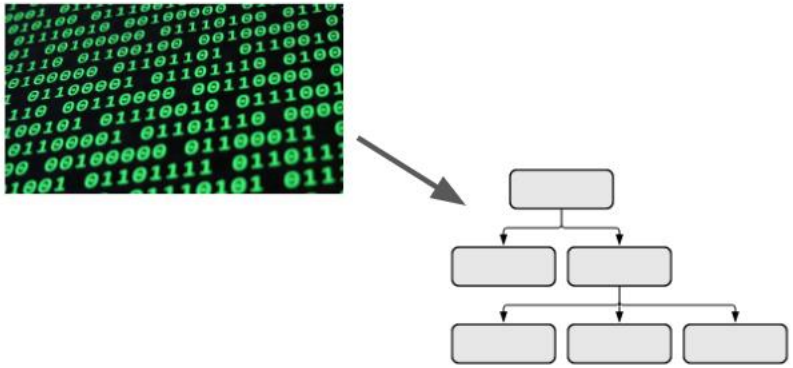
- Capture the knowledge of domain experts and allow it to be reused, shared and extended
- E.g., model of an autonomous sytem, or model of a red and black network





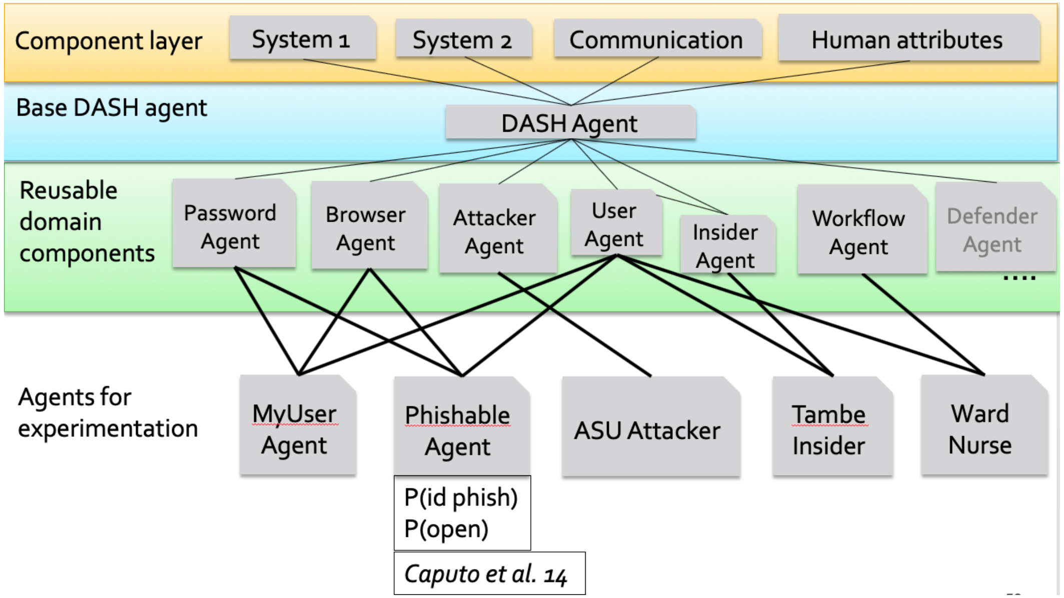
Reverse Engineering Binaries

- Help researchers bridge the semantic gap between binary code and source code
  - Binary – all malware and proprietary software
  - Source – understandable by humans
- Goal: usable abstractions for functional code representations
  - Approach: use ML to label binary code w functional descriptions



Library of Human Behavior Models

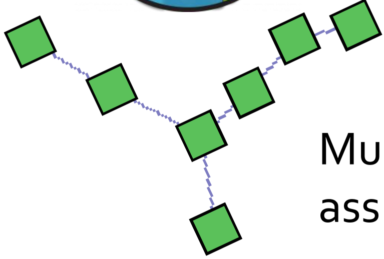
- Design experiments that include models of human user behavior
  - Rich models from psychology literature interact with attacks and defenses on DeterLab



Caputo et al. 14

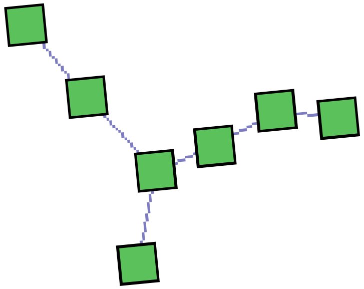
Dockerize Education Materials

5 K students
40 classes



Multiple nodes per assignment

Limited resources shared between researchers and students ~ 700 nodes



DREAMS

Personal copy for each user
No testbed resources needed
Consistent, long interaction
Customized assignments

Resource Reservations

- Current: FIFO, hold as long as needed
  - Many resources are held without being actively used
- Need for reservations
  - Demos, in-class use, tutorials, conf. deadlines
- Human-facilitated reservations are wasteful
- DREAMS reservations
  - Reserve specific resources for specific time
  - Per project quotas
  - Release resources that are unused at reservation time
  - All allocations for a limited time, can be extended if resources are available

Beyond DREAMS

Cybersecurity Experimentation of the Future (CEF)

Cybersecurity Experimentation of the Future (CEF): Catalyzing a New Generation of Experimental Cybersecurity Research

Community Plan and Roadmap to Develop Future Experimentation Infrastructure in Support of Cybersecurity Research

FINAL REPORT
July 31, 2015

- SRI and USC led Study
  - 75 stakeholders, 50 organizations
- 4 community engagement events
  - 81 people from 42 organizations

http://www.cyberexperimentation.org/report/

Need for Transformational Progress

Transformational progress in three distinct, synergistic areas:

1) Experimental methodologies and techniques
   - complex systems and human-technical interactions
   - **science of cyberexperimentation**
2) Rapid and effective sharing of data and knowledge and information synthesis
   - accelerate multi-discipline and cross-organizational knowledge generation and community building
3) Advanced experimental infrastructure capabilities and accessibility

Thank You

- Questions? Comments?
  - Terry Benzel (benzel@isi.edu)
  - Jelena Mirkovic (sunshine@isi.edu)