Revitalizing Cyber-Security Education Through Competitions

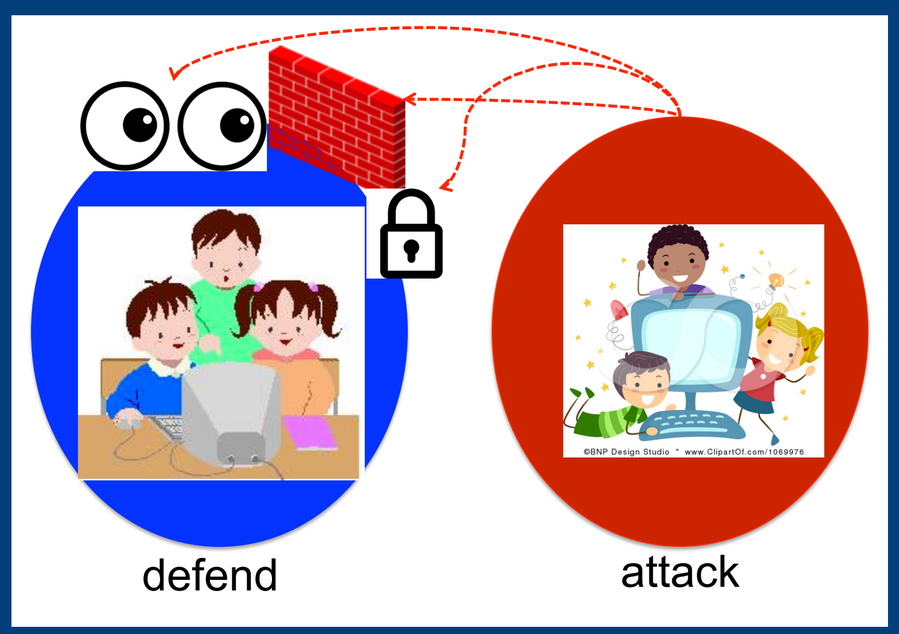

Dr. Jelena Mirkovic Dr. Ronald Pike

Cybersecurity is **adversarial** field, with attackers and defenders constantly trying to outsmart each other. Current security education does not capture this adversarial dynamics. Many classes are taught with just textbooks. Some classes include practical homework exercises. These help students acquire practical skills but do not teach them critical thinking or how to handle adversarial situations.

Problems with the existing education approaches:

- **Lectures only**: passive learning, low student engagement and retention
- **Hands-on homeworks:** teach skills but not critical or adversarial thinking
- **Regular competitions**: require solid knowledge and skills to enter, humbling experience for many

Our class capture-the-flag exercises teach critical and adversarial thinking to students in beginner cybersecurity classes. They help students internalize concepts learned in class, and reason about pros and cons of different defensive actions.



CCTFs teach students:

- Adversarial thinking
- Reasoning between offense or defense alternatives
- Importance of system/service monitoring
- Teamwork
- Testing and documentation
- Distributed systems

CCTFs

Feature	CCTF
Preparation	A few weeks
Duration	2 h
Topic	Intrusions, DDoS, DNS, BGP, crypto…
Team roles	Both Blue and Red
Occurrence	2-3 times per semester
Difficulty	Intermediate

Each CCTF is followed by a post-mortem, where groups share what they did and what they think happened in the competition. This is an opportunity for everyone to learn about successful offense/ defense strategies.

We modified the DeterLab's user interface to ease competition organization:

- Allocation/deallocation of multiple experiments with the same topology and settings
- Team creation and team assignment
- Access control so that offense/defense teams can only access certain nodes on the same experiment
- Automated scoring

Current Status:

- Five competitions developed to date:
  - Intrusions
  - DDoS
  - Cryptography
  - BGP
  - Secure coding
- Used in USC cybersecurity classes and by CSU Pomona in outreach activities
- Publicly released on DeterLab's sharing portal

Next Steps:

- Five more competitions are under development
- Develop team matching user interface to enable teams from different institutions to have scheduled competitions
- Evaluate student learning

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

ISI Information Sciences Institute
STEEL Security Research Lab@ISI
USC University of Southern California