Argonne National Laboratory's Cyber Defense Competition – Defending Tomorrow's Infrastructure Today

Name

Company

Contact info

1. ABSTRACT

The Cyber Security Workforce continues to experience shortages. Finding professionals with the skills to keep pace with the constantly-changing landscape is a challenge faced by all. Argonne has built, in cooperation with federal and industrial partners, a Cyber Defense Competition program with competing universities from across the country for the purpose of attacking this problem head-on.

The presenter describes the problem and explains what the project is about

2. BACKGROUND AND RELATED WORK

Women are only roughly eleven percent of the information security workforce.[1] With the current cyber labor shortage, women have a large opportunity to join the workforce. Numerous programs have been developed to help high school girls learn more about cyber security. Argonne National Laboratory has decided to continue the education of cyber security to college students through our Cyber Defense Competition. This competition seeks college students from varying levels of higher education and regions within the United States to defend a real-world simulation of an energy and water distribution system. This year's goal is to increase the amount of female participants within the university teams.

Teams are given a month to design and build a secure network comprising elements of information technology, a power grid, and a water processing system within the parameters of the competition scenario. They then come together for a two-day competition where they must complete their network and defend it from a team of attacking security professionals, while ensuring delivery of services to their customers. This model is unique in its combination of design & setup of a real network with a live-fire exercise to determine both security and usability.

Argonne National Laboratory's Cyber Operations, Analysis and Research (COAR) team partnered with Argonne's Education group is hosting the second Annual Cyber Defense Competition on Saturday, April 1, 2017 at Argonne National Laboratory.

In subsequent years, this event is intended to expand to a multi-laboratory virtual competition to allow for increased participation by students and laboratories alike. Increased emphasis will be placed on research and innovation, with plans to encompass a symposium for students to present their techniques. Teams will be increasingly incentivized through selection and scoring to think outside the box and demonstrate novel defensive methods.

This competition has seen huge success in driving excitement in students for cyber security careers, and giving them hands-on experience in a simulated real-world situation. It serves as the foundation for a talent pool that participating institutions can recruit from, and a testbed for new ideas that laboratories may wish to adopt or explore further. National Laboratories participating through attendance, providing security professionals to help test or attack the teams, or attending the co-located workshop directly benefit from this environment through the wealth of new ideas and networking opportunities provided.

A Cyber Defense Competition (CDC) is a competition that focuses on the defensive/hardening nature of cyber security. A typical CDC has a Blue Team (defenders) that protects a network infrastructure from the Red Team (attackers). A blue team consists of high school or college students who secure and harden their competition system. A red team consists of students or industry professionals that work to cause cyber destruction to the blue teams' network infrastructures. The competition is scored utilizing a point system. Points can be both given and taken away depending

on the actions or lack of action from both blue and red teams. The blue team with the most points at the end of the competition is declared the winner of the event.

The presenter explains how the competition is different from others

3. APPROACH AND UNIQUENESS

Argonne's CDC has added some elements to their competition that no other competition has. Some of the unique differences in Argonne's CDC include:

- Argonne's CDC has a Green Team. The green team simulates that of an actual user of the systems being defended by the blue teams and attacked by the red team. The objective of having a green team is to enforce a real-world instance of balancing usability with security. Scoring from the green team is subjective includes: accessibility, ease of system, and usability.
- A Pink team will be introduced into Argonne's CDC to work alongside the red team. The pink team is comprised of individuals that are interested in learning the theory and technical skills behind the red team. The pink team will have an educational component in which the volunteers will not only get to see what red team is doing but understand what blue teams are defending as well.
- A large difference between Argonne's CDC and other hosted CDCs is the addition of the physical realm to the competitions. Most competitions simulate a real network but the physical impacts cannot be seen. The goal of Argonne's competition was to make it as real world scenario for the competing teams allowing them to have a cyber network but also allow for a physical impact to occur. To accomplish this goal, a miniature, but physical and functional infrastructure replica is provided to each blue team during the competition. If the infrastructure replica is involved in a cyber-attack, the teams will see the physical replicas reacting to the attacks in real time.

4. RESULTS AND CONTRIBUTIONS

Last year this included eight teams from two states & around 20 volunteers. This year participation had to be capped at 15 teams from nine states (with 27 teams having applied to compete) and over 100 volunteers!

Argonne's first annual CDC took an electrical grid/infrastructure approach. The competition scenario was centered on the ability of the blue teams securing their networked environment along with their "electrical grid". The "electrical grid" was represented with an LED light that was wired up and placed inside a small wooden birdhouse that was given to each of the Blue teams. When the team's light went out it was a good indication that the red team had successfully been able to breach that team's network infrastructure.

Argonne's second annual CDC will bring the competitors much closer to the cyber-physical realm. This year will consist of both the electrical and water infrastructures being combined into one competition environment. The blue teams will have to secure their networked systems and industrial control systems (ICSs) in order to "keep the lights on" and "keep the water running". The water will have LED lights and be colored so participants and guests can easily tell if there is a stoppage.

The results of the first competition are explained, and the expected results of the next competition are presented

5. REFERENCES

Morgan, S. (2016, March 28). *Calling All Women: The Cybersecurity Field Needs You And There's A Million Jobs Waiting*. Retrieved from Forbes: https://www.forbes.com/sites/stevemorgan/2016/03/28/calling-all-women-the-cybersecurity-field-needs-you/#19101d26381c