Changing the Future of Cybersecurity

Author: Jessica MacMillan

With increasingly complicated systems that need to be secured, effective trainings for the next generation of cyber professionals is essential. The California Cyber Innovation Challenge allows students to participate in a training challenge environment that is engaging and stimulating. Cybersecurity roles take 20% longer to fill than standard IT jobs, so the CCIC aims to help train some of the next generation’s cybersecurity professionals. The challenge exists not only as a training for cybersecurity skills, but also leadership, critical thinking and communication. Students enter the CCIC in teams and must work together on a series of both physical and digital challenges.

The CCIC began in 2016, with Cal Poly running it since 2017, and has been growing steadily every year. At the 2019 challenge, there were over 150 high school and junior high students in attendance with 26 teams from 21 different schools across California. Figure 1 shows a heat map of the participants’ locations, and there has been a steady increase in team representation across California. Each challenge also engages Cal Poly faculty, staff, and students to help design and execute the entire event. This event receives a great deal of attention from the State of California Government, CSU, UC, military, and the vendor community. Cal Poly is viewed as a leader in bringing “Learn by Doing” into the State and National cybersecurity discussion.

Immersive environments are implemented to be extensions of the narrative each team is placed in. For the 2019 challenge, there was an attack on a pacemaker, so the immersive environments were an apartment, a hospital room (shown in figure 2), an admin office, as well as a box of police documents. The goal of the physical elements is to push the students in their critical thinking and communication skills through solving a series of escape room-like puzzles. All of the physical challenges lead to digital evidence, cell phones, flash drives, computer hard drives, etc. Once the team completes the physical challenges, they then analyze the digital evidence to try to understand who committed the crime for that given scenario, and how it was executed. At the end of the challenge, each team has to present their findings to a panel of judges. This helps train the students in presentation skills and being able to articulate their thoughts into a concise presentation.

The 2018 and 2019 challenges were medically themed challenges with issues of random ware and weaponized proximity attacks as the central focus. The demonstration of this effective training allowed for a collaboration with DEF CON 27’s Biohacking village to further the training on cybersecurity in the medical industry.

Next year, the event will continue to grow and will be out of this world. Space, satellites, and cybersecurity are at the national forefront of discussions. The commercialization of space increases cybersecurity concerns for both the public and private sectors. The 2020 competition will feature a live-immersive environment at Cal Poly’s digital range located at Camp San Luis Obispo. Students will respond to a fictional storyline of a satellite that was hacked and falls to Earth. Students will be engaged in multiple hands-on, space-themed set designs to solve the cyber mystery of how the satellite was hacked. The CCIC will continue its efforts to grow the cybersecurity workforce and develop an aware and educated public.