UC SANTA BARBARA

THE Current

August 24, 2016

Sonia Fernandez

Cyber-Gladiators

One hundred and four teams. Two years. Three winners. One intense competition. UC Santa Barbara's resident hackers, team Shellphish, pitted their skills against cyber-security experts across the country to become one of the top teams in the 2016 Defense Advanced Research Projects Agency's (DARPA) Cyber Grand Challenge (CGC). The 13-member group of computer science graduate students emerged third overall, taking $750,000 in addition to the $750,000 cash prize they won for qualifying for the finals in Las Vegas.

"The Shellphish team did great considering that it was the only academic team in the top-three positions," said faculty advisor and computer science professor Giovanni Vigna. The top two teams, ForAllSecure and TechX, have academic origins but have spent years in industry.

Shellphish almost didn't compete, and the road to Vegas was full of fits and starts, making their win especially significant.

"There were big, huge arguments between us," Ruoyu "Fish" Wang said of their 2014 decision to join the DARPA contest. "Basically, we are a research team; we were not really sure how the competition was going to contribute to our research." Add to that the effort and time involved, funding they would have to generate and the fact that they were relatively late to the party, other teams having had the federal funding and research for years prior to the CGC.

Not that Shellphish wasn't familiar with the competition's "capture-the-flag" (CTF) format. A standard test of the cyber-security skills of its participants, the exercise requires teams to defend their own home-base of servers from exploits conducted by other teams, while seeking out the chinks in their competitors' armor. Shellphish's continuously evolving roster of members also organize the annual UCSB International Capture the Flag contest, the world's largest and longest-running educational hacking competition.

What made the CGC different, however, was that instead of a contest in which hackers analyze, attack and defend in real time, the combat would, for the first time ever, take place between autonomous bots. Participants would build systems preprogrammed to compete in a sort of cyber-gladiator tournament, without any human involvement. All the work had to be done before the actual competition.

Unwilling to pass up the opportunity to flex some cyber-security muscle and earn serious bragging rights, Shellphish sent in their registration just a few minutes before the deadline.

And then they procrastinated. For almost a year.

"It was like, 'Oh yeah, I'm going to start working after this project deadline,'" said Shellphish hacker Antonio Bianchi. "And then after the next, and then after the next…'" Before they knew it, the deadline for the qualification round was upon them. They kicked into high gear for two and a half weeks, barely squeaking into the final round.

"We weren't expecting that," he said.

You'd think after the close calls the team already had with CGC deadlines, they'd have learned their lesson and gotten cracking on the final competition, with the knowledge that other world-class hacker teams were — presumably — hard at work creating the Cyber-security Robot of the Future. Think about it: With the Internet of Things emerging and virtually every aspect of our lives online and automated, providing cyber-security — already difficult under the best of circumstances — could become much more challenging. The sheer amount of data and devices on the network would multiply the chances of a large-scale disruption, whether through an unintentional hardware bug, or worse, a malicious program.

“Detecting exploitation, patching and reverse-engineering bugs and understanding whether they are bugs are still human-labor intensive and everything is getting significantly more dependent on software,” team member Kevin Borgolte said. Cyber-security experts have conducted exhaustive research on best practices, he added, but there has been little integration.

Fast-forward to earlier this year, to the run-up to the CGC finals in July. Teams had been tweeting their progress for months and making plans for the final event — which this year was held alongside the fabled DEF CON hacking conference — and finishing their robots.

As for Shellphish?

“For the final event, of course, we took it a little bit more seriously,” said Borgolte. “We started two months before the competition … so that’s at least a factor of four, possibly six, from the last time.”

The work was a frenzy of analysis, engineering and strategy. Every component had to work efficiently and reliably. Once the bot was deployed, there was no touching it. The lab became the team’s second home. Members found that their individual skills and research interests played well into the creation of their bot Mechanical Phish.

“We had all been doing research and playing CTFs,” said Aravind Machiry. “We were already doing a lot of the stuff that we used for CGC.”

On the day of the finals, the team wasn’t obligated to be in Las Vegas; the contest was completely automatic. But the stakes were high, and this was the first competition of its kind. They would not have missed it for anything in the world. And it was in Vegas.

“Of course we were going to go,” said Chris Salls.

It was a spectacle, the team said. The components were on stage with translucent cooling pipes, protected by an air gap and guards. While the teams had nothing to do but wait while the machines cranked out their programs, live commentators played up the tension by asking participants to comment on their progress. With no running tally to watch, the sleepless team speculated on anything they could: How did the contest count points? Were they correct in their strategy? Did a dip in their components’ temperatures mean something had stalled?

Eight agonizing hours later Shellphish got their preliminary answer: Third Place.

“It felt pretty good, but we kind of predicted that we would get at least top three,” said Nick Stevens. They might have done better, he said, if it wasn’t for something of a snafu in the beginning, in which they aggressively detected and patched all vulnerabilities in their services.

“One reason we decided to patch everything is because in the human version of the game everything does get exploited,” he explained. In the automated version, only a fraction of the vulnerabilities in their system was actually attacked — perhaps a window into the hacking landscape of the future, in which cyber-security experts would have to become more surgical with decisions to take down services in order to fix them. Though simplified for the contest, these problems could play out in real life as more of us rely on smart devices and systems.

So, game over, bragging rights attained, right? Wrong.

They woke up the next morning after a night of partying (because Vegas), expecting to prepare for the award ceremony … only to find an email calling for a special meeting.

“Of course we saw it an hour too late,” said Borgolte, “and our captain sprinted to the room, but it was in another hotel, so he sprinted to the other place where the other people were.” According to the competition organizers, external verification could not confirm their result and it looked like the nominal fourth place team could take Shellphish’s spot. And so began the most gut-wrenching part of the competition for the team.

“We were so distracted and exhausted,” said Salls. For two days the team was kept in the dark as the contest organizers examined the data and decided to extract it again for analysis.

“We were speculating that this was a bug that we caused,” said Borgolte. The re-analysis revealed that yes, Shellphish had indeed come in third.

Their placement made official, team Shellphish is now tying up a couple of loose ends before resuming regular programming. The software behind Mechanical Phish was recently open-sourced at developer website GitHub, and the team is writing their CGC post-mortem.

“We have to write up a report for CGC, which is due on the 25th of this month,” said Bianchi, “so we’ll probably do it on the 25th.”

About UC Santa Barbara

The University of California, Santa Barbara is a leading research institution that also provides a comprehensive liberal arts learning experience. Our academic community of faculty, students, and staff is characterized by a culture of interdisciplinary collaboration that is responsive to the needs of our multicultural and global society. All of this takes place within a living and learning environment like no other, as we draw inspiration from the beauty and resources of our extraordinary location at the edge of the Pacific Ocean.