UC SANTA BARBARA

THE Current

December 11, 2013
Sonia Fernandez

Spy vs Spy

While people were busy last Friday bundling up, going holiday shopping or winding down a long week with some friends, the world was at war. Countries across the globe raced to be the first to launch attacks and cut down their opponents while factions in each nation plotted against each other, seeking out weaknesses and mercilessly destroying each other with mechanical precision. Old rivalries and memories of battles lost were resurrected in the ultimate contest for survival and domination.

For Giovanni Vigna, UC Santa Barbara professor of computer science, it was just another day at work. This time, he was overseeing the annual International Capture The Flag (iCTF) contest, the world's largest online computer hacking competition.

"Think, if you could do this for a good cause, how much good you could do," said Vigna, who specializes in Internet security.

But world domination is more fun. So from 8 a.m. to 5 p.m., he and his cohort of students and assistants, the architects behind this game of mass destruction, were busy monitoring the various systems set up for the teams of hackers participating in the contest. More than 1,300 participants in 120 teams — all students at academic institutions — gathered at laptops, desktops and workstations worldwide in a bid to attack, defend and emerge victoriously to push the big red button of annihilation.

Born out of an end-of-term exercise in which Vigna's students were pitted against each other to exploit network vulnerabilities, the iCTF has since blossomed into a

full-fledged international hacking contest, complete with bragging rights and the occasional monetary prize. Fueled by coffee, bagels and pizza, Vigna and his crew run a system of services that doles out points to those teams capable of defending their territory against attacks, and credits to those who manage to mount a successful attack. The winner, ultimately, is the best defender, but credits allow teams to wreak havoc upon each other by financing bids that could upset the playing field, by supplying arms, for instance, or sabotaging another team.

Early iterations of this 10-year-old competition were versions of the classic “capture the flag” scenario, in which one team bypassed another’s security system to obtain the “flag” associated with the service.

As the competition grew — and as the cybersecurity problems of the real world increased — so did the complexity (and sometimes the absurdity) of the game. In past years hacker teams were racing to steal money from a fictional hillbilly bank, or attack a rogue nation led by an evil mastermind. Last year their mission was to disrupt each other’s SCADA systems — the industrial control systems that monitor and control big infrastructure processes like water treatment or delivery, power generation and other utilities — plunging each other into the Dark Ages. Alliances are not allowed; neither are attacks on the game’s system. That will earn the miscreant team instant cyber death.

Fun and games aside, this contest serves a very serious and timely purpose.

“The basic idea of this mission is cyber situational awareness,” said Vigna. “It reflects the fact that not all the resources in a network have the same importance.” Sponsored by the U.S. Department of Defense, the purpose of this exercise is to understand how to prioritize efforts toward the protection of more important aspects of the network, the hierarchy of which changes as the game evolves.

“By doing this, we force people to think more closely about the game and be very surgical in protection and attack,” Vigna said. The most valuable learning comes from the months of preparation participants undergo before the competition, in which students think about security and design programs that enhance the protection of their service. Recent large-scale network breaches and security debacles serve as endless fodder for consideration. Recently the game has been modified so that attacks and exploits were sent to Vigna’s crew to execute, a move that has provided valuable data and insight on hacker strategies.

Cyber situational awareness is one of the qualities Vigna and his colleagues in the UCSB Computer Security Group (CSG) are looking to study and enhance in their work as more sensitive information comes online in the world, and attempts to gain this information become more sophisticated.

“Right now what we’re seeing increasingly is this concept of advanced persistent threats,” said Vigna. “These are malware that infect machines and stay hidden for a long time.” Instead of the clunkier, indiscriminate mass attacks, these threats target certain high-value entities for information, from state secrets to bank account passwords. In 2009 the CSG, composed of Vigna, computer science professor Christopher Kruegel and led by computer science professor Richard Kemmerer, successfully conducted their own real-life exploit by taking control of an advanced botnet called Torpig that was able not only to steal sensitive information but also alter data in the infected computer while circumventing antivirus programs.

UCSB can’t pump out computer security experts fast enough for the “insane” demand, said Vigna, mainly because Internet security is one of those “black-or-white” sciences.

“You can’t be 80 percent secure. If you’re not fully secure, you are catastrophically not secure,” he said.

Last Friday the pendulum swung wildly as the balance of power tipped from one continent to another. By 10 a.m., the reputedly friendly and harmonious Canadians were first in line to hurl the world into oblivion. However by late afternoon the Russians were proving that the spirit of the Cold War was alive and well by taking several top spots, while the rest of the world watched — and possibly hoped — that internecine conflict between team Bushwhackers (Russia) and powerhouse MoreSmokedLeetChicken (also Russia) would somehow open a gap of opportunity. Meanwhile, Carnegie Mellon University team PPP, which won last year’s contest, was off in the boonies. Team DelusionsofGrandeur, out of the U.S. Air Force Academy, was doing an impressive job in the top four, but it was team SpamAndHex out of Hungary that impressed Vigna the most.

“Wow, that’s new,” he said, commenting on their 11th-hour shot to number 2. No stranger to surprises, Vigna got one of his own when his service, written in Swahili to confuse intruders, became vulnerable when an undergrad on the UCSB hacking team in the next room decoded it with the help of Google Chrome. In another

situation last year, an overload of users paralyzed the game itself with a major meltdown. This year, the competition’s organizers were prepared.

“No Healthcare.gov problems here,” Vigna quipped.

At the end of the day it was the Eastern Europeans — Bushwhackers and SpamAndHex — that had the dubious honor of winning the global arms race. The rest of the teams, no doubt woozy from too much caffeine, sugar and staring at lines of code, made their final announcements through the Internet relayed chat service, before calling it a day and falling asleep to dreams of their next chance to rule the world.

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.