Focus

The 2010 International Capture the Flag Competition

Giovanni Vigna
University of California, Santa Barbara

The iCTF is a security competition—a one-day, live hacking event that happens each December. It has evolved over the years from a dozen or so universities to nearly 70, with approximately 900 people playing at one time. This year differed slightly from previous years—*IEEE Security & Privacy* and Adobe offered cash prizes, and the competition featured different designs than in the past.

Brian Pak is an undergrad student at Carnegie Mellon University and leader of the Plaid Parliament of Pwning, the team that won the 2010 International Capture the Flag Competition organized by Giovanni Vigna every year. Giovanni Vigna talks with Brian about the competition.

Giovanni Vigna: Brian, can you tell us how you found out about the iCTF and how you got involved in it?

Brian Pak: PPP [Plaid Parliament of Pwning] looks for every possible capture-the-flag competition that it can participate in. We encountered the iCTF last year and got fourth place overall, first place in the US. This year, the iCTF came along again, we entered again, and this time we got first place.

Vigna: Tell me a little bit about how the PPP group was created.

Pak: It was originally formed in Fall 2009, so it's a fairly new group. CMU didn't have any hacking teams. I was doing research under David Brumley, and he suggested creating a team, so I did. We only had about five people in our group when it started, and I was the only undergrad. Now we have about 15 active members, half undergrad and half graduate, so it's fairly well balanced.

Vigna: How did you guys prepare for the iCTF?

Pak: Basically, we went over previous editions of the iCTF, because some of them are released publicly, to see how each year's iCTF was structured and what we needed to code beforehand—for example, what kind of tools we needed and what kind of scripts might be useful for the competition.

Vigna: This year, all the participating teams were attacking the rogue nation of Litya, an anagram of Italy, which was run by a ruthless dictator who supported cybercrime. The goal of all the teams was to stop this nation from its cybercriminal activities, with a [subfocus] on situational awareness—the idea of attacking a service when it's most useful. Every team was given a description of the various activities carried out by the nation of Litya, and the attackers had to compromise services at a particular time, when they were most needed, sort of a surgical attack. In addition, if you were detected by Litya's intrusion detection system, which was a SNORT filter, you would be cut off from the competition for awhile. Brian, what were the most challenging parts of the competition for your team?

Pak: Since we were deducted for attacking the wrong services at the wrong time, it was really critical to know exactly what services we were allowed to attack. Figuring that out was the most challenging part because the mission was given as hand-written Petri nets. We had a group of graduate students who created a tool that could figure out which state we were in based on the transitions that we were given at certain points. The best thing about this tool is that they coded

 1540-7993/11/$26.00 © 2011 IEEE

it in type-safe functional programming language.

Vigna: That's exactly what we were trying to have people do, but not many people got to the point of having a tool that did it. Did you guys have a specific strategy?

Pak: Since the SNORT filter was publicly available, we actually tested it. We had it on our side, and if it matched any of the packets, we just dropped back and didn't send them. So…

Vigna: …So this would prevent you from sending something that would eventually hurt yourself in the competition?

Pak: Yes.

Vigna: Did you just focus on the target, or did you also try to attack other teams, which, by the way, was allowed?

Pak: Yes. While the services were down, we analyzed the given virtual machine, found a back door, and tried to log into other machines. This back door allowed us to connect to other machines—other teams' machines—and gain full access. We installed our SSH keys so we could connect back to their machines later, just in case we needed it. [We also corrupted] the scripts that run to check in with the mother ship so that [they would send] the wrong passkey. At the end, we tried to deduct other teams' points by submitting their flags for the wrong service.

Vigna: Yeah, I think that this part of the game was missed by some of the teams that got hurt pretty badly by other teams' attacks, but that's part of the game. I mean, nobody got really hurt, they just lost the competition.

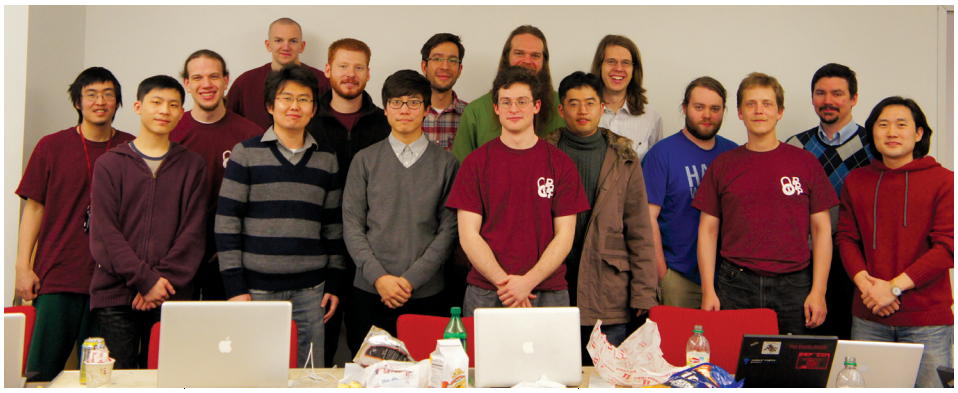
Pak: Some of the teams were very confused and didn't know why their points were taken off, but that's what happened.

Vigna: What skills do you think are the most important for participating in this kind of competition?

Pak: Our team members have their own skill sets, so we divided into three groups, one to solve side challenges to keep up on the network, the second to examine the target network and figure out the running services, and the third for exploiting the services to get points. Basically, we needed different skill sets to protect our own network, to exploit the services, and to break into other team's machines. Obviously, to solve side challenges you need to know a lot of things, you know?

Vigna: Ah, yes. The side challenges were puzzles that teams had to solve to get points—actually, to get money to bribe administrators. Going back slightly, you said that you wanted to participate in as many hacking competitions as possible. What is the value that you find in these competitions in general and the iCTF in particular?

Pak: Every time we participate, we learn a lot—we get hands-on experience. We study crypto, we study reverse engineering, but competitions are where we actually test and use them. The iCTF has all of the aspects we can test because it has side challenges as well as attacking and securing our own boxes. Some of the competitions require us to do write-ups after [the event] is done. Once we do the write-ups, we can publicize [our work], and people can learn from it—that's how we started learning when we partici-



Plaid Parliament of Pwning. The 2010 International Capture the Flag winning team hails from across Carnegie Mellon University. Brian Pak was the team's vulnerability analysis leader and David Brumley was the faculty sponsor. Team members (not all pictured here) include Sang Kil Cha, Jiyong Jang, Ed Schwartz, Tim Vidas, Thanassis Avgerinos, JongHyup Lee, Andrew Wesie, David Kohlbrenner, Chun Yu, Ricky Zhou, Hudson Thrift, Matthew Dickoff, Tyler Nighswander, Joseph Lee, Michael Stroucken, Ivan Jager, Spencer Whitman, and Rob Floodeen.

pated in competitions, by looking at other people's write-ups from previous years.

Vigna: So are you going to provide a write-up for this competition?

Pak: Some groups are really diligent and they document everything while they're solving problems. Our group is fairly lazy in that aspect. It's a lot of work. It's really fun while you're doing [a competition], but once it's over, everyone is tired. You can still check out the ones we wrote for other competitions at our team blog [http://ppp.cylab.cmu.edu].

Vigna: In the traditional capture-the-flag design pioneered at DEFCON, every team gets the same operating system with the same vulnerable services. The basic idea is that every team has to look at their services, find out where the vulnerabilities are, patch their own version of the operating system, and use the knowledge about this vulnerability to hack into all the other teams' operating systems and capture the "flags," which are data snippets associated with each different service. The iCTF followed that scheme between 2003 and 2007, but then in 2008, we started to introduce completely different designs. You participated in '09 and '10, so how do you think ours compared to the more traditional contest?

Pak: The iCTF is very unique, and it takes a lot of time to understand what's going on at first. PPP loved it—it has themes every year, and it sometimes reflects our current issues in some way. It's really fun compared to other traditional ones. I mean, traditional ones are fun, too, but they're the same every time. You get kind of bored, but with the iCTF, you don't know what's coming next.

Vigna: We aim to surprise with a curve ball every time, but it's getting harder and harder to come out with new designs. I can assure you that for 2011, we're thinking of something even crazier. We'll see if we'll be able to pull that out. One last question: How do you and your team plan to use the skills that you honed in these kind of contests after you graduate?

Pak: Some of us are graduating next semester and some are going to work, while others are going to pursue graduate school. It seems that some companies are very interested in our skill set, and I think that these skills these days are important anywhere. Everyone needs security.

Vigna: Do you have any big plans for the money that you won?

Pak: We have a contribution point system, so basically you get points whenever you contribute to our team. We have a study session every week and each member who is volunteering gives a lecture on some topic. At the end of the semester, we tally up these points and do a raffle. I think we might use this money to buy some prizes for next semester and still have fun. ☐

Giovanni Vigna *is a professor in the Department of Computer Science at the University of California, Santa Barbara. His current research interests include malware analysis, Web security, vulnerability assessment, and intrusion detection. He is known for organizing and running the world's largest inter-university capture-the-flag hacking contest, called iCTF, that attracts dozens of institutions around the world every year. Vigna has an MS with honors and a PhD from Politecnico di Milano, Italy. He is a member of IEEE and the ACM. Contact him at vigna@cs.ucsb.edu.*