Washington Post Live

The ethics of Hacking 101

Brian Pak, left, founder of a recreational hacker team called PPP, made up of current and former Carnegie Mellon students, participates in the DefCon 22 "Capture the Flag competition in Las Vegas. His team won. (Ashkan Soltani/For The Washington Post)

By Ellen Nakashima and Ashkan Soltani October 7

At the University of Tulsa, professor Sujeet Shenoi is teaching students how to hack into oil pipelines and electric power plants.

At Carnegie Mellon University in Pittsburgh, professor David Brumley is instructing students on how to write software to break into computer networks.

And George Hotz, a largely self-taught hacker who became a millionaire in part by finding flaws in Apple and other computer systems, is now back in school, where he's one of the stars on Carnegie Mellon's competitive hacking team.

Cybersecurity: A Special Report

Shenoi, Brumley and Hotz are players in a controversial

area of technology: the teaching and practice of what is loosely called “cyberoffense.” In a world in which businesses, the military and governments rely on computer systems that are potentially vulnerable, having the ability to break into those systems provides a strategic advantage.

Unsurprisingly, ethics is a big issue in this field. Both professors say they build an ethics component into their curriculum; Shenoi won’t even accept students who don’t promise to work, if hired, for the National Security Agency, the Energy Department or another U.S. government agency.

But some experts say the academic community is not taking ethics seriously enough, and professors are not accepting responsibility for the potentially dangerous skills they are teaching.

The very nature of hacking means that a lot of its skills and standards evolve outside academia. (Hotz, known in tech circles by the handle “geohot,” says he learned most of what he knows on the Internet “and from playing with things.”) This leads advocates of teaching cyberoffense to say that the “good guys” have to keep up — which in turn raises more questions about whether such education is morally right.

“There’s a very large stigma around saying we do anything offense-related,” said Tyler Nighswander, 23, a computer science graduate student at Carnegie Mellon. “It’s certainly understandable that you don’t want to say

your school teaches offense — 'Oh, you mean you teach kids how to break into computers and steal stuff?' "

Some academics note that it may be too late to stop the worldwide expansion of offensive cyber tools and techniques.

"There is an escalating arms race in cyberspace as governments, companies and malicious actors are all going on the offensive, most of it under a shroud of secrecy and absent any meaningful political oversight," said Ron Deibert, director of the University of Toronto's Citizen Lab.

Seeking 'vulnerabilities'

No more than a handful of professors have the knowledge and resources to teach cyberattack skills at the level of Brumley or Shenoi, whose students are heavily recruited for government and industry positions.

At Tulsa, Shenoi, 54, obtains permission from energy companies for his students to attempt to hack into them, infiltrating the systems that run gas pipelines or power grids and gaining access to critical U.S. infrastructure. They also do penetration testing for other companies, finding "vulnerabilities," or flaws, that enemy hackers could exploit.

"We have a class where we teach people how to write things like Stuxnet," Shenoi said, referring to a computer worm, reportedly developed by U.S. and Israeli scientists, that was found in 2010 and damaged about

1,000 centrifuges in an Iranian uranium-enrichment plant, delaying the country's nuclear program. Stuxnet, whose deployment is often considered the first true use of a cyberweapon, was built around an unprecedented four "zero-day exploits" — that is, attack tools based on previously unknown software flaws.

Shenoi began teaching courses on offensive computer techniques in 1999, he said, and by 2008, Tulsa was offering an entire program. Now, he said, there are "four courses in reverse engineering, two in cyber operations, two in offensive SCADA [supervisory control and data acquisition], and one on malware analysis and creation."

Shenoi said that the potential power of offensive cyber techniques is so great that he accepts only students who intend to work for the government and who have records that would qualify them for government security clearances. He interviews all the applicants as well as their parents. He sends 15 to 20 students a year, he said, to work at the NSA or the CIA.

"In order for me to teach these real-world attack skills, these students have to be trusted," he said. "They cannot go to work for the private sector.

"There's no reason to teach private-sector people how to use Stinger missiles," he continued. Similarly, he said, you don't teach them to use cyber weapons.

Brumley, 39, has taught offensive cyber skills since 2009. A self-described "patriot," he says he discusses

ethics in his classes at Carnegie Mellon — an introductory computer security course as well as more advanced vulnerability analysis, in which students learn techniques for breaking through computer defenses. Some of Brumley's students work for the government, but most go to start-ups, big companies such as Google or defense contractors.

To develop their skills, Brumley encourages his students to compete in hacking contests. In August, a recreational team he advises called PPP, made up of about 20 current and former Carnegie Mellon students, won the ultimate U.S. showcase of hacking skills at the DefCon hacking conference in Las Vegas — a "capture-the-flag" competition in which 20 teams tried to break into one another's computers.

PPP's top gun is Hotz, who gained fame in 2007 for "jailbreaking" the previously impenetrable iPhone. He left Carnegie Mellon as a 23-year-old sophomore to work on his own, and is now back as a junior at 25. Hotz is so skilled that he has won some contests solo — as in July, when he beat nine teams to win $30,000 at the SecuInside competition in Seoul. He earned $200,000 in April for finding bugs in Google's Chromebook computer and the Firefox browser. Brumley calls him "a machine." Hotz boasts that he is "maybe the best hacker in the world."

A question of profit

Obviously, these students are developing valuable skills.

Shenoi says his students never make money off the vulnerabilities they discover or exploits they develop. They give the information for free to the companies whose systems they are testing, or to the government. Intelligence agency officials fly every so often to Tulsa to be briefed on the flaws the students have found.

Brumley agrees that it is dangerous to share vulnerabilities or exploits with anyone but the software vendor or the U.S. government.

“If you’re selling exploits in a free market,” he said, “then you’re potentially selling them to the adversary.”

Nighswander, a former student of Brumley’s, said that he has never sold a vulnerability to a software vendor, but that he thinks it’s ethical to do so, saying, “When you think that finding a vulnerability can take weeks and months, you can understand that the person wants to get compensated.”

Hotz declined to say whether he has sold an exploit (although he was caught last year on a surreptitiously recorded conversation appearing to broker a $350,000 deal to sell exploits to jailbreak the iPhone to a Chinese company).

“I have never worked with any country aside from the U.S.,” he said. He says he doesn’t dwell on issues of morality, saying, “I’m not big on ethics.”

Brian Pak, 25, who created the PPP hacking team while

studying under Brumley and now works for a start-up he cofounded, said that sometimes, noodling around on his own, he finds bugs in software and discloses them to the software vendor. He said he has never sold information about flaws, although some vendors offer “bounties” of up to several thousand dollars. He holds onto some vulnerabilities for use in research — a practice common among security researchers, he said.

“I also don’t think it’s unethical to provide vulnerabilities or exploits to the U.S. government,” Pak said. “I trust the U.S. government. The government protects me. As long as it’s not used against our own people, I see less of an issue.”

But some experts disapprove of providing previously unknown or “zero day” vulnerabilities to the government — whether for free or for profit. They worry that, rather than disclosing these zero days to vendors, the government is stockpiling them for use against adversaries. Doing so would leave the software vendors ignorant of dangerous flaws in their products, making the Internet less secure, they say. They also charge that the government is using these tools with far too little public debate, for example, in the controversial area of domestic law enforcement.

Christopher Soghoian, chief technologist for the American Civil Liberties Union, said the government should have a policy of promptly disclosing any bugs it discovers so that software companies such as Microsoft

can fix them before they cause damage. Not doing so can undermine network security, he said.

But Brumley said such a blanket policy would be unwise.

“The obvious example is Stuxnet,” which destroyed Iranian centrifuges, he said. That, he said, was “an opportunity to use an exploit for good.”

“Twenty years earlier, that would be the thing that we flew in bombers and bombed factories for, and people would die,” he said.

Dual-use tools

Selling exploits and vulnerabilities is not illegal, per se, but selling them with the intent that they’ll be used to hack someone else’s computer is a crime. Software is a classic “dual use” product. It can be used to do something as innocuous as unlock an iPhone to allow consumers to switch providers or as destructive as causing an adversary’s nuclear centrifuges to spin out of control.

Some academics say the teaching of hacking techniques should remain limited.

“I’m personally against the widespread or wholesale teaching of offensive cyber,” said Arthur Conklin, associate professor of information and logistics technology at the University of Houston. For one thing, he said, vetting students for trustworthiness, as Shenoi does, would be impractical on a mass scale.

Giovanni Vigna, a computer science professor at the University of California at Santa Barbara, warned that not teaching offensive skills is "not a very smart option because the bad guys are going to develop them anyway." He added, "The key is to make the students understand what are the lines that cannot be crossed." So he integrates into his courses on offensive cyber "a very substantial chapter on ethical issues."

Some experts argue that the government should regulate the sale and use of offensive cyber technology — but others, including Shenoi, say regulation will only drive the market for such products deeper underground. At this point, the U.S. government is in the process of placing export controls on some hacking and surveillance tools. It already has forbidden the sale of such technologies to countries with particularly egregious human rights records, such as Sudan and Iran.

Meanwhile, interest in offensive cyber skills is growing. Experts estimate that several thousand personnel in private industry work at finding bugs and building exploits. More companies are training employees in offensive skills, and more people are competing in hacking competitions.

In this context, Soghoian of the ACLU fears that universities are teaching students high-end skills without a solid ethical foundation.

"The academic computer security community has not yet realized the role they are playing in cyberwar," he said.

Shenoi said that, above all, he wants to impress upon his students the responsibilities that come with their technological prowess.

“They have great power to do harm. They have power to intimidate. They have power to accrue money illegally,” he said. “What I tell them is, ‘You may be learning some potentially deadly skills. But use them gently and wisely, and use them for the good of society.’ ”

Related:

Key to keeping cyberspace safe? International accord.

With mobile devices, many firms are playing Russian roulette with cybersecurity

What top government and business officials are saying about cybersecurity