The United States Cyber Challenge

A national competition and talent search to find and develop 10,000 cyber security specialists to help the United States regain the lead in cyberspace.

5/8/09

The web pages for the US Cyber Challenge will be posted on May 29 at www.sans.org/uscc and at other sites. To learn more about the program prior to May 29, email USCC@sans.org

Outline

1. The Need
2. The Competition and Skills Programs
3. The Sponsorship

1. The Need

In the 1950s and 1960s, Sputnik and the space race inspired young people to pursue careers in science and engineering. The average age of NASA's Mission Control during the Apollo 17 Mission, for example, was 26. We have a similar opportunity to inspire today's young people to tackle the important challenges we face, including cyber security. Seizing this opportunity is crucial, because the US is falling behind other countries in cyber security skills development because other countries have made this a national priority and have implemented national talent searches.

A good illustration, the story of one young man (data provided by iDefense), comes from China.

> *Tan Dailin was a graduate student at Sichuan University when he was noticed (for attacking a Japanese site) by the People's Liberation Army (PLA) in the summer of 2005. He was invited to participate in a PLA-sponsored hacking contest and won. He subsequently participated in a one-month, 16-hour-per-day training program where he and the other students simulated various cyber invasion methods, built dozens of hacking exploits, and developed various hacking tactics and strategies. He was chosen for the Sichuan regional team to compete against teams from Yunnan, Guizhou, Tibet, and Chongqing Military Districts. His team again ranked number one and he won a cash prize of 20,000 RMB.*
>
> *Then, under the pseudonym Wicked Rose, he formed a group called Network Crack Program Hacker (NCPH) and recruited other talented hackers from his school. He found a funding source (an unknown benefactor) and started attacking US sites. After an initial round of successful attacks, his funding was tripled. All through 2006, NCPH built sophisticated rootkits and launched a barrage of attacks against multiple US government agencies. By the end of July, 2006, NCPH had created some 35 different attack variants for one MS Office vulnerability. During the testing phase, NCPH used Word document vulnerabilities. They switched to Excel and later to PowerPoint vulnerabilities. The result of all of this activity is that the NCPH group siphoned thousands, if not millions, of unclassified US government documents back to China.*

What steps is the United States taking to meet this challenge?

The one point that elicits broad agreement is that a critical shortage exists in technical cyber security skills.

> *"The cyber threat to the United States affects all aspects of society, business, and government, but there is neither a broad cadre of cyber experts nor an established cyber career field to build upon, particularly within the Federal Government. [Using an] airplane analogy, we have a shortage of 'pilots' (and 'ground crews' to support them) for cyberspace." (**Center for Strategic and International Studies, Report of the Commission on Cybersecurity for the 44th Presidency, December 2008)***
>
> *"The provisioning of adequate cyber forces to execute our assigned missions remains our greatest need." **(Gen. Kevin P. Chilton, Commander, U.S. Strategic Command, March 17, 2009, in testimony before the House Armed Services Committee**)*
>
> *"I cannot get the technical security people I need." (**Gen. Charles Croome, Commander, Joint Task Force - Global Network Operations, in response to a question from a CSIS Commissioner asking what is the most critical problem he faces in meeting the growing cyber challenge. May 28, 2008)***
>
> *"There are about 1,000 security people in the US who have the specialized security skills to operate effectively in cyberspace. We need 10,000 to 30,000." **(Jim Gosler, Sandia Fellow, NSA Visiting Scientist, and the founding Director of the CIA's Clandestine Information Technology Office, October 3, 2008.)***

Shortages extend from the Federal Government to the US defense industrial base, federal information systems contractors, utilities, telecommunications companies, and most other segments of the critical national infrastructure. In fact, wherever senior management has been made aware of a major, damaging cyber attack, the shortage becomes immediate and acute. Every week more US organizations are experiencing the pain of sophisticated cyber attacks.

Sadly, there is no shortage of talent on the malicious attacker side of the equation. The US Cyber Challenge provides a critical and necessary path to divert those that may go to the dark side.

2. The Competition and Skills Development Programs

The US Cyber Challenge is a national talent search *and* skills development program. Its purpose is to find 10,000 young Americans with the interests and skills to fill the ranks of cyber security practitioners, researchers, and warriors. Some will, we hope, become the top guns in cyber security. The program will nurture and develop their skills, and enable them to get access to advanced education and exercises, and where appropriate, enable them to be recognized by employers where their skills can be of the greatest value to the nation.

Young people in America have enormous technical aptitude and a powerful desire to find careers that make a difference. Those drawn to the field of cyber security are motivated by a variety of reasons. Some young people choose cyber security because they are looking for a challenge; others want a job that offers good economic prospects; and still others want to solve computer crime, or better yet, help avoid it. And some want to serve in the military using their cyber skills.

The United States Cyber Challenge will cast a wide net to enable young people who are capable and willing to demonstrate their skills and then develop those skills far beyond what would have been possible had they not been identified early.

The identification process relies on national competitions – with many winners.

Three large-scale competitions are envisioned:

For high school students

(1) *CyberPatriot*, The High School Cyber Defense Competition conducted by the Air Force Association: a competition in computer system and network defense - where the competitors attempt to analyze the security state of the competition network and then must secure the systems while maintaining services and responding to attacks by a hostile Red Team. This is a preparatory program that encourages students to continue their security training in college and to compete in the National Collegiate Cyber Defense Competition.

For the top high school students and for college and graduate students

(2) The DC3 Digital Forensics Challenge conducted by the DoD Cyber Crime Center (DC3): a competition in digital forensics where, in increasingly challenging scenarios, contestants attempt to uncover evidence on digital media, just like you see on all of the crime scene investigative shows on TV. Whether it is an intrusion by a nation state or a child pornography investigation, digital forensics is the key to answering the who, what, where, when, why, and how questions.

(3) The Network Attack Competition conducted by the SANS Institute: a competition in network vulnerability discovery and exploitation. This program will include substantial ethical and legal instruction. An essential tenet of the emerging US national strategy for cyber security is that offense must inform defense. Perhaps the single most important reason that America's computers are so easily exploited is that the government and the companies in the critical infrastructure relied for security guidance on individuals who were not intimately familiar with how cyber attacks work.

Promising candidates will be immediately recognized and will be invited to attend regional "camps" at local colleges, run jointly by college faculty and cyber security experts from the community, where they will develop their skills more fully and participate in additional competitions. The students who rise to the top in these regional programs will be invited to live national challenges like those conducted by schools coordinated by the University of Texas at San Antonio and NYU Polytechnic.

Greatly promising candidates from these programs will be given either Federal Service grants or SANS Institute scholarships to study advanced cyber security programs and may earn scholarships to colleges and graduate programs at participating schools.

Finally, the best of the candidates will be brought into federal agencies like the National Security Agency, the FBI, DoD DC3, US-CERT, and US Department of Energy Laboratories, all of which are helping to make this program effective.

To enable employers to find promising candidates, the program will include a web site where outstanding candidates from this challenge and other related challenges are illuminated with profiles in common, easy-to-assess formats. No names will be provided to ensure candidate privacy, but when reputable employers find candidates they want, the candidates will be given the opportunity to connect with the employer.

3. The Sponsorship

The Cyber Challenge will be announced on May 29, 2009 as part of the follow-on activities of the CSIS Commission on Cybersecurity for the 44th Presidency and will be managed under CSIS oversight. The pilot competitions are being funded by the Defense Cyber Crime Center (Forensics Challenge); the Air Force Association, the University of Texas at San Antonio and SAIC (*CyberPatriot Defense Competition*); and the SANS Institute (Network Attack Competition) . Over time, the funding will begin to come from a combination of entry fees, like those used in the National Robotics Competition, and government and corporate sponsorship by organizations that will gain from a radical increase in the number and quality of cyber security experts.