Editors: Matt Bishop, bishop@cs.ucdavis.edu
Cynthia Irvine, irvine@nps.edu

Hacking Competitions and Their Untapped Potential for Security Education

Gregory Conti, Thomas Babbitt, and John Nelson
US Military Academy

Information security educators can learn much from the hacker community. The word "hacker" is controversial, and the idea of emulating this community is problematic to some. However, we use the term in its purest form: individuals who creatively explore technology and push it in new directions. Because of this imaginative, playful spirit, most hacker conferences sponsor diverse and intense competitions, many organized by the attendees themselves and facilitated via the conference organizers. These competitions test participants' ingenuity and problem-solving skills, are fun and innovative, and draw large, enthusiastic groups of participants and spectators.

Academia and the computer security industry have widely adopted hacker competitions, such as DEF CON's Capture the Flag (CTF), to augment information security education. Many other hacker competitions, however, are less known. Here we examine these untapped competitions' potential and identify those that can energize and enhance information security education in both the classroom and the industry.

Over the past decade, educators have increasingly realized the value of the hacker mindset for teaching information security.[1–3] By learning the hacker perspective and considering the unanticipated use of technology, students will be better prepared to deter attacks and defend against them. They'll also be more able to perform ethical hacking activities, such as penetration testing, reverse engineering, and active network defense.

Types of Competitions

Hacker competitions touch on many aspects of computer science, information technology, electrical engineering, and information security education. They're powerful ways to teach, inspire, build teams, recruit students, and facilitate advanced skill building. Competitions can also build the reputation of participating individuals and institutions.

We researched the competitions of major hacker conferences, including DEF CON, CanSecWest, ToorCon, ShmooCon, HOPE (Hackers on Planet Earth), and the Chaos Communication Congress. Addressing all the competitions these conferences host is beyond this article's scope. We instead highlight a spectrum of competition techniques that have distinct pedagogical merit and are readily translatable to the classroom environment.

Network Warfare

Perhaps the best-known competition in the hacker community is CTF, which challenges participants to attack and defend computing resources while solving complex technical problems. Run by security experts including DDTek, Kenshoto, and the Ghetto Hackers, CTF has been an important catalyst for research, innovation, and government, academic, and industry collaboration. CTF variants have emerged, such as the Collegiate Cyber Defense Competition and the US National Security Agency-sponsored Cyber Defense Exercise.[4] CTF has even spawned a business model in which White Wolf Security and other firms host similar exercises for third parties. Innovation in CTF events occurs continually. For example, PacketWars competitions operate like a spectator sport. (For URLs for PacketWars and other competitions mentioned in this article, see the sidebar.)

Every rigorous information security education program, whether technically or policy focused, should include appropriately scoped CTF competitions to avoid a significant knowledge gap in its graduates.

Wireless

Wireless-networking technologies are on the rise, and wireless vulnerabilities and open access points

 1540-7993/11/$26.00 © 2011 IEEE

are increasingly common. Hacker competitions highlight these concerns. For example, war-driving competitions, during which participants map open access points, quantitatively illustrate the prevalence of insecure system configurations and raise public awareness. Competitions have spurred new antenna designs and illustrated that consumer-grade wireless-network transmissions are vulnerable at extreme distances. To explore the implications of RFID tracking and social networking, the HOPE conference issued electronic badges to volunteers, captured location and demographic data, and facilitated attendee-developed projects for display. Facilitators then submitted this dataset to Dartmouth's Crawdad wireless research dataset repository, illustrating potential second- and third-order research benefits from hacker competitions.

Educators can use wireless-hacking events to emphasize many learning objectives, such as ethics, privacy rights, antenna design, networking protocols, and the importance of usable security.

Related URLs

- **Badge Hacking Contest,** www.defcon.org/html/defcon-18/dc-18-contest-results.html#dc18badgehack
- **Collegiate Cyber Defense Competition,** www.nationalccdc.org
- **Crack Me if You Can,** http://contest.korelogic.com
- **Crawdad,** http://crawdad.org
- **Cyber Crime Center Digital Forensics Challenge,** www.dc3.mil/challenge/2011
- **Dual Core,** http://dualcoremusic.com/nerdcore
- **Hack Fortress,** www.shmoocon.org/hack_fortress
- **HOPE (Hackers on Planet Earth) conference badges,** http://amd.hope.net
- **IEEE Conference on Visual Analytics Science and Technology (VAST) Challenge,** http://hcil.cs.umd.edu/localphp/hcil/vast11
- **International Collegiate Programming Contest,** http://cm.baylor.edu/welcome.icpc
- **International Olympiad in Informatics,** http://ioinformatics.org/index.shtml
- **Open Backdoor Hiding & Finding Contest,** https://backdoorhiding.appspot.com
- **PacketWars,** http://packetwars.com
- **PWN2OWN,** http://dvlabs.tippingpoint.com/blog/2011/02/02/pwn2own-2011
- **Social Engineering Capture the Flag,** www.social-engineer.org/defcon-social-engineering-contest
- **ToorCon Tamper Evident Contest,** http://sandiego.toorcon.org/index.php?option=com_content&task=section&id=11&Itemid=27

Cryptanalysis

Code-breaking competitions attract significant interest while providing a deeper learning of cryptography. The US Cyber Command created a buzz around its organization by embedding a code into its logo.[5] The US Central Intelligence Agency's Kryptos sculpture draws intense attention from amateur and professional code breakers, and even numerous pop culture references.[6] Hacker conferences use cryptographic competitions to great effect. ShmooCon and ToorCon badges have included subtle codes, puzzles, and clues. Other conferences have disseminated code-breaking contest sheets to attendees and awarded prizes at their closing ceremonies.

Importantly, some competitions require winners to share their techniques for the benefit of all. DEF CON's Crack Me if You Can hash-cracking competition challenges participants to illustrate weaknesses in the username/password paradigm by working backward from hashes to passwords.

Cryptographic competitions complement code-breaking assignments. Educators can also employ them more broadly outside the classroom to facilitate recruiting, enhance Information Security Day activities, inspire self-learning, and exercise problem-solving skills.

Hardware Hacking

Many security compromises occur when adversaries attack hardware devices in unconventional ways. Hardware-hacking competitions challenge hackers to build novel devices and modify existing hardware to behave in similarly unanticipated ways. An excellent example is DEF CON's Badge Hacking Contest. Attendees receive a modifiable electronic badge. DEF CON provides software tools for altering the badge's firmware and facilities with tools and parts for modifying and testing the hardware. Attendees have converted their badges into such devices as a barcode emulator, breathalyzer, and social-network analyzer. Robotics challenges at hacker and other conferences are also popular.

At West Point, we've found that hands-on hardware-hacking activities, often drawn from *Make* magazine and Joe Grand's ideas,[7] are highly rewarding for students at all skill levels.

Secure Coding and Malicious Software

Attacks have recently increased against end-user application software, including Web browsers, word processors, and document viewers. One long-term solution is to teach secure coding practices that eliminate many vulnerabilities early during software development, instead of dealing with them through postdiscovery patches. Although the ACM's International

Collegiate Programming Contest and the International Olympiad in Informatics facilitate development of programming and algorithm skills, they don't focus on securing the resultant programs from attack. Conversely, some hacker competitions focus on the implications of secure software development and antivirus technologies. For example, Core Security has sponsored the Open Backdoor Hiding & Finding Contest, highlighting the difficulty in detecting backdoors despite open source code. DEF CON's Race to Zero contest challenged contestants to modify malicious code samples to bypass antivirus software, while still maintaining a functional payload.[8] This contest helped determine the real-world difficulty of avoiding detection by different classes of antivirus software. Considering how a hacker forces a system to fail while it's being built is challenging but highly educational.[3]

Educators can use the competition models we just described, along with their variants, as informal classroom demonstrations. Or, they can use these models more formally as active components of an information security curriculum.

Social Engineering

A social engineer influences people to divulge sensitive information and manipulates their actions. Hacker conferences feature demonstrations such as social engineering by telephone and conduct scavenger hunts forcing teams to acquire various items through human manipulation.

Recently, DEF CON initiated the Social Engineering CTF, in which participants passively gather information on a target company before the conference. During DEF CON, participants gather specific target information during a 20-minute attack. The contest rules deliberately avoid violating the law and victimizing anyone.

Properly constructed social-engineering competitions are accessible to a wide range of students. Using forethought and creativity, educators could use human-centric competitions to great educational benefit. One example could be a phishing email writing contest during which students design (without sending) messages to entice recipients to open attachments or divulge information. Exercises such as these enable students to better appreciate the human component of an increasingly technological world.

Physical Security

Information security education often overlooks physical security. Rigorous network, system, and application safeguards matter little if an attacker gains physical access to information systems, storage devices, or network infrastructure. Hacker conferences hold competitions in lock picking, which employ scenarios in which the participant must escape from simulated captivity—that is, handcuffs, a cell, and a locked door. Another example is ToorCon's Tamper Evident Contest, which challenges participants to bypass purportedly tamper-resistant technologies, thus testing vendor security claims. Matt Blaze illustrated why computer scientists should study safecracking to enhance security metrics and understand why security systems fail.[9] We agree and argue that physical-security competitions are practical methods for information security students to better understand security vulnerabilities when an attacker gains physical access to a device.

The Arts

An important component of an information security curriculum is effectively communicating technical security and privacy principles, including to a non-tech-savvy public. For example, the band Dual Core has reached broad audiences with its high-energy security-and-privacy-oriented music. Even Snoop Dogg is helping to fight cybercrime by working with Symantec's Norton on the Hack is Wack cybercrime rap contest.[10] Hacker conferences frequently sponsor design competitions, placing the winner's designs online and on T-shirts, conference badges, and signage. These competitions also invite interdisciplinary collaboration, such as an information security program partnering with a local art school to obtain graphic-design support.

Again, creative adoption of these practices into the classroom environment can reap valuable pedagogical rewards, as long as educators clearly define the desired learning outcomes.

Other Types

We encourage you to search online for other hacker competitions you could apply to your curriculum. Of course, exciting and educational competition ideas aren't just born to hackers. One example is the US Department of Defense Cyber Crime Center Digital Forensics Challenge, which you could adopt to teach computer forensics. Another is the IEEE Conference on Visual Analytics Science and Technology (VAST) Challenge, which poses challenging research questions and provides data for analysis. Even LAN parties, a hacker conference staple, can become a powerful educational tool. We've used them as social events to attract members for our information security club, while teaching networking fundamentals to our frequently nontechnical participants. ShmooCon's Hack Fortress competition combines hacker and gamer teams. A success in either a gaming or hacking challenge gives an advantage to team members competing in the other domain.

Incentivizing Participation

Hacking competitions attract many participants simply because they're exciting and thought-provoking. However, many competitions also include prizes and public recognition at closing ceremonies. For example, CanSecWest's PWN2OWN competition challenges competitors to break into target systems, with the first successful team winning the machine.

Academia has greater resource constraints. However, we can incentivize participation in numerous cost-effective ways. Avoiding onerous rules while encouraging innovation and excitement stimulates learning; integrating competition into the curriculum and awarding performance points also motivate students. Books are a low-cost but valued prize. Awardees might also receive public recognition through media coverage and sharing photographs and videos of the event through social media. This outreach also spotlights the larger program and informs the public about information security principles.

Setting the Proper Ethical Tone and Context

The hacking contests we've described are edgy, dual-use activities that can lead to good or evil. Despite the dangers, the learning outcomes far outweigh the risks. Instructors must emphasize that responsibility accompanies skills and knowledge, and they must discuss improper behavior and reprimand students who display it. As we know, some students might consider using these skills for malicious activities; the occasional student will act upon these urges. To counter this temptation, the teacher must set the proper ethical tone for each activity and across the entire curriculum, ensuring that all students respect these necessary limitations on their activities.

Hacking competitions can help educators infuse learning and excitement into information security education programs. Successful instructors will carefully consider their learning objectives, set the proper ethical tone and context, and motivate participation. A carefully constructed and challenging competition will attract many participants.

Hacker conferences are a rich source of innovation. A diverse set of artifacts is available online, which you can employ as training aids to illustrate key learning objectives and gain ideas for constructing your own competitions. The hacker competition scene is dynamic, so continue to monitor conference websites for the latest developments. Even better, participate in these contests yourself, encourage your students to do so, organize new ones, and join this large, vibrant community. □

Acknowledgments

The views in this article are the authors' and don't reflect the official policy or position of the US Military Academy, the Department of the Army, the Department of Defense, or the US government.

References

1. S. Bratus, "What Hackers Learn That the Rest of Us Don't: Notes on Hacker Curriculum," *IEEE Security & Privacy*, vol. 5, no. 4, 2007, pp. 72–75.
2. G. Conti, "Why Computer Scientists Should Attend Hacker Conferences," *Comm. ACM*, vol. 48, no. 3, 2005, pp. 23–24.
3. M. Locasto, "Helping Students Own Their Own Code," *IEEE Security & Privacy*, vol. 7, no. 3, 2009, pp. 53–56.
4. W. Adams et al., "Collective Views of the NSA/CSS Cyber Defense Exercise on Curricula and Learning Objectives," *Proc. 2nd Conf. Cyber Security Experimentation and Test*, Usenix Assoc., 2009, p. 2.
5. N. Shachtman, "Crack the Code in Cyber Command's Logo," blog, 7 July 2010; www.wired.com/dangerroom/2010/07/solve-the-mystery-code-in-cyber-commands-logo.
6. K. Zetter, "Solving the Enigma of Kryptos," Wired.com, 21 Jan. 2005; www.wired.com/culture/lifestyle/news/2005/01/66334.
7. J. Grand, "Research Lessons from Hardware Hacking," *Comm. ACM*, vol. 49, no. 6, 2006, pp. 44–49.
8. R. Lemos, "Mandiant Researchers Win Race to Zero," *SecurityFocus*, 11 Aug. 2008; www.securityfocus.com/brief/795.
9. M. Blaze, *Safecracking for the Computer Scientist*, tech. report, Dept. of Computer and Information Science, Univ. of Pennsylvania, 2004.
10. M. Lennon, "Snoop Dogg Joins the War on Cybercrime," *SecurityWeek*, 1 Sept. 2010; www.securityweek.com/snoop-dogg-teams-norton-fight-cybercrime.

Gregory Conti *is an assistant professor in the US Military Academy's Department of Electrical Engineering and Computer Science and is responsible for the academy's information security education program. Contact him at gregory.conti@usma.edu.*

Thomas Babbitt *is an instructor in the US Military Academy's Department of Electrical Engineering and Computer Science. Contact him at thomas.babbitt@usma.edu.*

John Nelson *is an assistant professor in the US Military Academy's Department of English and Philosophy. Contact him at john.nelson@usma.edu.*