Rebecca Slayton looks at efforts to blend, certify and market the subversive skills of hacking with the ethos of professionalism.

the PARADOXICAL AUTHORITY *of the* CERTIFIED ETHICAL HACKER

IN JULY 2013, the front page of *The New York Times* reported that Edward Snowden was a Certified Ethical Hacker (CEH). The *Times* noted that the certification process would have "given him some of the skills he needed to rummage undetected through N.S.A. (National Security Agency) computer systems and gather the highly classified surveillance documents that he leaked last month" (Drew and Shane 2013).

The founders of the CEH credential quickly distanced themselves from Snowden's actions, noting that CEHs were required to follow a code of ethics, and that only one had previously lost a certification for disclosing confidential information (Drew and Shane 2013). By contrast, Indian papers were proud of the revelation that Snowden had received training in Delhi. The *Times of India* reported, "The hacker who shook the US intelligence machinery and had world leaders railing against the United States for spying on them picked up crucial skills in India" (Phadnis 2013:1). To undermine the U.S. intelligence machinery, it implied, was also to demonstrate technical mastery.

These responses illustrate a tension within the CEH credential: it sought to appropriate the technical savvy associated with hackers and the U.S. military and intelligence agencies while distancing itself from the untrustworthy and morally suspect image of hacking. In this essay I show how these tensions animated the early development and popular reception of the CEH credential. I argue that the certification did not represent the professionalization of ethical hacking—a field that had already existed for decades—so much as it did an effort to certify and market a blend of hacker skills and professional ethics.

I first describe how anxieties about hackers and the ethics of skilled information technology workers fostered the rise of information security certifications in the 1990s. I next discuss the establishment and early popularization of the CEH, showing how the credential sought to appropriate the technical authority and

mystique of hackers and the U.S. military without the stigma of the popular association of hackers with criminal activity. I then discuss how the authority and credibility of the certification was ultimately limited by the tension between the goals of professionalism—to standardize and authorize knowledge practices—and the creative and subversive spirit of hacking.

THE RISE OF INFORMATION SECURITY CERTIFICATIONS

Early efforts to establish information security certifications grew out of the audit community, and were modeled on the Certified Public Accountant. William Murray, a leader in the Electronic Data Processing (EDP) Auditors society, recalls first suggesting the idea in the mid-1980s, as hackers began making news headlines: "We were experiencing the same problems that have confronted every emerging profession including how to separate the professionals from the amateurs. It was particularly important for us because of the amateur, i.e., 'hacker,' culture that surrounded so much of what we do" (Murray 2003:76).

In 1989, the EDP Auditors society joined with other professional computing organizations to create the International Information Systems Security Certification Consortium, or $(ISC)^2$, a new organization dedicated solely to establishing a certification in information security. Over the next several years, $(ISC)^2$ developed the Certified Information Systems Security Professional (CISSP) exam, which was finally launched in 1994.

CISSP provided a broad, business-oriented perspective on security; it was based on 17 different "specialty areas," which included access control methods, regulatory and legal issues, cryptography, policy development, and "information ethics" (Tipton 1993). Importantly, certification also required that members swear to uphold the $(ISC)^2$ code of ethics.

For many employers, the CISSP served not only to educate workers, but also to "civilize" highly skilled technical people by assuring their ethical intentions and suitability for business. For example, Steve Akridge spent 20 years in the Navy and retired in 1995 as a chief cryptologist, but industry employers wanted him "to prove he could address bottom-line problems and direct large operations security outside the military" (Dugan 2001:36). Organizations interested in "ethical hacking" services also expressed a preference for CISSP-credentialed contractors because "CISSPs must take a vow to adhere to a high code of ethics that includes reporting unlawful activities" (Messner 1999:25).

While CISSP focused on deep technical skills, the System Administration, Networking and Security (SANS) Institute began developing a set of Global Information Assurance Certifications (GIAC) around 2000. By the early 2000s, CISSP was the best-known certification, followed by GIAC, but additional certifications were proliferating. As of late October 2003, *Certification Magazine* reported 56 vendor-neutral and 20 vendor-related security certifications. As the magazine reported, "IT [information technology] professionals seeking information security certifications have an embarrassment of riches to choose from" (Tittel 2004: 28).

ESTABLISHING THE CERTIFIED ETHICAL HACKER

The CEH credential grew out of this burgeoning economy of information security certifications. Ethical hacking had been a professional pursuit since at least the mid-1960s, when the U.S. military and other organizations began using "red teams" or "penetration testers" to attempt computer security breaches, and thereby help in identifying and mitigating vulnerabilities. However, the CEH credential was not directed primarily toward penetration testers, but rather toward any professionals who could benefit from learning to think like a hacker. It distinguished itself from other certifications by the promise of a proactive rather than a reactive approach to security, wherein organizations could anticipate and prevent breaches instead of constantly recovering from and planning around their most recent breach.

The first organization to offer CEH training was Intense School, a company established in 1997 by two brothers and IT consultants, David and Barry Kaufmann, and their cousin, Ron Rubens. As the name suggests, Intense School offered "boot camps" in information technology, and in the late 1990s, it began offering training for CISSP. However, it found the $(ISC)^2$ certifying body difficult to work with, so with the help of some hackers with military experience, it developed an ethical hacker certification (Ron Rubens, personal communication, October 23, 2016). After attending a federal information technology trade show in 2003, the new certification began attracting publicity. As *Washington Technology* reported: "When hackers go bad, they bust into your Web site and wreak havoc. But when they go good... they may very well come from Intense School" (Socha 2003).

The founders of Intense School were not the only ones to see the appeal of the CEH. In response to the terrorist attacks of September 11, 2001, Jay Bavisi, a legal professional trained in Britain, led the establishment of the International Council of E-Commerce Consultants, or EC-Council, to help certify professionals who could protect against attacks on electronic commerce. By 2003 it was offering the "Certified Ethical Hacker" certification (https://www.eccouncil.org/about/). Rather than establishing entirely new schools, the EC-Council became a certifier of training courses and exams, mobilizing entrepreneurs in the information security training business. Rubens recalled that Intense School wanted to focus on training rather than building up the credibility associated with a certification (Ron Rubens, personal communication, October 23, 2016). By 2009, Intense School was recognized by EC-Council as the "#1 Authorized Training Center in North America" (http://www.intenseschool.com/about/). EC-Council's strategy allowed the Ethical Hacker certification to expand rapidly, and by 2007 CEH courses were offered in more than 60 countries.

Paradoxically, the international spread of the credential resulted from the intensely local nature of training. Although some companies did begin offering online training—for example a "midnight hacking" course provided a "quick overview"—geographically specific boot camps provided the more in-depth training (Paulson 2006:3). In June 2003, *Forbes* signed up one of its tech reporters for the ethical hacker boot camp, and in the fall, she reported on her experience in a course held at a Comfort Inn in the Washington, DC, suburbs. She described the instructor as a "20-year veteran of the Canadian military" who was a "jovial version of a drill sergeant" (Schoenberger 2003: 119) Her class consisted of 18 men and 2 women from both private and government organizations, including the Army, Air Force, Department of Commerce, Microsoft, and other private sector firms (many of which were government contractors).

Military patrons were a crucial source of authority for the CEH credential.

Advertisements for CEH certification programs.

Announcing its certification in 2003, Intense School noted that it had been training defense department and National Security Agency workers for 18 months (Swartz 2003). It also hired former military professionals as instructors. While its "boot camp" style of training was not unique—other IT training programs were similarly structured around "all-inclusive" packages that covered lodging, food, and training—the boot camp also simulated elements of hacker sociality, such as marathon hacking sessions that kept students up all night, fueled by piles of junk food.

COMPUTERS

Hacking Goes Legit

Corporations are using "tiger teams" and less glamorous methods to check computer security.

BY ANN STEFFORA AND MARTIN CHEEK

"TIGER TEAMS," THE TERM WAS MADE POPULAR IN the 1992 movie *Sneakers* in which Robert Redford and his cohorts were hired by corporations such as banks and insurance companies to find weaknesses in computer security by actually breaking into a system. Although it's controversial, executives are finding that data-penetration services such as "tiger teams" are a way to test the security that information-technology (IT) departments are supposed to provide. Companies, including American Express, Monsanto, and the Philadelphia Savings Fund Society, have taken advantage of hacker-like services. But are they an effective method of preventing security risks?

Currently, reported U.S. losses resulting from penetration by hackers are running $150 billion to $300 billion a year. Some companies do not report their losses, fearing damage to their corporate reputation, possible loss of competitiveness, and loss of customers' and stockholders' confidence, says Winn Schwartau, executive director of INTER.PACT, a security consulting firm in Seminole, Fla. He also serves as an analyst for the National Computer Security Assn., Carlisle, Pa.

The consultant points to a bank in Atlanta, which loses an average of $20 million a year in ATM fraud and internal employee pilfering, rather than report the loss at the location where it occurs. The loss is allocated among all departments, so each takes part of the hit.

Security for corporations has become such a hot issue that even hackers have crossed the line and offered their penetration services to corporations. For example, two years ago a group of hackers called the Legion of Doom decided to go legit.

Three members of the hacking group joined with a former securities trader to form a Houston-based company to help clients keep unwanted invaders out of their computer systems. Called Comsec Data Security, it claimed to have three *Fortune* 500 companies for clients.

Comsec believed its experienced hackers gave it a unique perspective in developing better security systems for companies. "We know how hackers hack, what motivates them, and how they think," Scott Chasin, one of the founding directors, said in the first days of

INDUSTRY WEEK, FEBRUARY 7, 1994
43

Industry Week February 7, 1994, p. 43.

CERTIFICATION VERSUS "REAL WORLD" EXPERIENCE

While the ethical hacker certification sought to appropriate the authority of hackers and the military, many hackers gave it little credence. For example, Pieter "Mudge" Zatko, a hacker who also worked on security for a Department of Defense contractor, suggested that ethical hacker certifications could be used to "weed out job candidates," but that they didn't teach real-life experience: "Certification courses teach you about buffer overflows and Microsoft hacking tools—stuff that's already well known and rudimentary and then you get a hacker title. It doesn't mean you have a strong grasp of security" (Leung 2005: 47).

The real skills of hacking were portrayed as resistant and even opposed to institutionalization. Marc Maiffret, a hacker who co-founded eEye Digital Security in 1998, stated: "Typically hackers are people who didn't finish college because they were so into finishing [their hacking] project. I didn't finish high school and there are people here who have PhDs in computer science who learned hacking on the side" (Leung 2005: 47). One professional who held the CEH label among other certifications acknowledged this point: "Real world experience and knowledge are what will carry the day. The best hackers are not the certified ones, but are the ones that are doing it for real and normally do not poke their heads up too often. Be practical, not certified" (Bort, 2008). Asked about the ethical hacker certification in 2003, one "black-hat" hacker wrote: "Some 'IT pros' may find a few techniques to secure against well-known attacks, but the underground is always 10 steps ahead" (Swartz 2003).

Proponents of certification also acknowledged the derivative nature of such training in their responses to the question often posed to ethical hacking schools: Couldn't the training be turned to nefarious purposes? Aaron Cohen, founder of the "Hacker Academy" in Chicago, said, "Hackers don't need our help" (Paulson 2006:3). Furthermore, Cohen and his lead instructor, Ralph Echemendia, argued that it was important to learn from "black-hat" hackers. Echemendia, who had learned hacking as a teenager and went on to teach for Intense School, argued against the view that "if you associate with hackers you can't be a certified professional." He ran an underground hacker meeting where participants remained relatively anonymous, explaining that he got "real-world" information from them and occasionally tried turning them to legal hacking (Paulson 2006:3).

At the same time, training centers also felt pressure to distance themselves from the underground world of illegal hacking. When Intense School engaged the notorious hacker and social engineer Kevin Mitnick to help with one of its courses, certain companies threatened to cut their ties with the training program. Partly to satisfy their customers, and partly out of an uneasy sense that Mitnick might be an untrustworthy partner, they did not continue working with him (Ron Rubens, personal communication, October 23, 2016).

CONCLUSION

Professional institutions and standards have historically been offered as a substitute for the interpersonal trust that becomes infeasible in a large and geographically dispersed field (Porter 1996; Shapin 1995). Something similar was at work with ethical hacker certifications in the early new millennium. As governments and corporations moved their operations online, demand for "ethical hackers" rose sharply, as did demand for means of demonstrating their trustworthiness.

But contrary to what theories of professionalization might suggest (Abbott, 1988), the ethical hacker certification did not come from penetration testers seeking to control entry to their field of work. In fact, the certification was not aimed primarily at people interested in becoming full-time penetration testers, but rather at any professional who could benefit from learning to "think like a hacker." Rather than representing the professionalization of ethical hacking, the certification emerged as a means by which entrepreneurs could capture a particular market niche in the rapidly growing business of information security certifications. The certification promised to meld a professional ethos with the technical prowess of hackers.

While this melding was persuasive to many, the tension between the subversive skills of hacking and the standardizing aims of professional certification ultimately limited the authority of the credential. Hackers were quick to recommend being "practical, not certified." And while U.S. military agencies implicitly endorsed the certification by sending some of its personnel to be trained, neither the Department of Defense nor civilian agencies ever granted the certification the monopoly powers enjoyed by organizations such as the American Medical Association. Certification became a valuable currency for jobseekers, but it continued to derive its credibility from the darker and more mysterious worlds of the military and hacking. ■

REBECCA SLAYTON *is Associate Professor jointly in the Science & Technology Studies Department and the Judith Reppy Institute for Peace and Conflict Studies.*

BIBLIOGRAPHY

Abbott, Andrew. 1988. *The System of Professions: An Essay on the Division of Expert Labor.* Chicago: The University of Chicago Press.

Bort, Julie. 2008. "Security Certs, Vampires and Dumpster Diving." *Network World*, April 10. link.

Drew, Christopher, and Scott Shane. 2013. "Résumé Shows Snowden Honed Hacking Skills." *The New York Times*, July 4. Available at link.

Dugan, Sean. 2001. "Certifiably Secured." *InfoWorld*, July 9, p. 36.

Leung, Linda. 2005. "Hackers for Hire." *Network World*, June 20, p. 47.

Messmer, Ellen. 1999. "Could You Pass This Tough Security Test?" *Network World*, March 15, p. 25.

Murray, William H. 2013. Oral history interview with William H. Murray. Charles Babbage Institute. Retrieved from the University of Minnesota Digital Conservancy. Available at link. P 76.

Paulson, Amanda. 2006. "New Academy Teaches 'Ethical Hacking.'" *Christian Science Monitor*, December 13, p. 3.

Phadnis, Shilpa. 2013. "Snowden Honed Hacking Skills in Delhi." *Times of India*, December 4, p. 1.

Porter, Theodore. 1996. *Trust in Numbers.* Princeton, NJ: Princeton University Press.

Schoenberger, Chana. 2003. "A Week at Hacker Camp." *Forbes*, September 15, 119–120.

Shapin, Steven. 1995. "Trust, Honesty and the Authority of Science." In *Society's Choices: Social and Ethical Decision Making in Biomedicine*, edited by Ruth Ellen Bulger, Elizabeth Meyer Bobby, and Harvey V. Fineberg (pp. 388–408). Washington, DC: National Academies Press.

Socha, Evamarie C. 2003. "Survival Guide: Ron Rubens, CFO and COO, Intense School." *WashingtonTechnology.com*, April 17. Available at link.

Swartz, Jon. 2003. "Tech Pros Get to Know Their Enemy." *USAToday.com*, September 23. Available at link.

Tipton, Hal. 1993. "Certification of Security Practitioners." *Information Systems Security* 1(4): 75–84.

Tittel, Ed. 2004. "Building a Career in Information Security." *Certification Magazine*, April, pp. 28–31, 48.