Pretending that Systems Are Secure

S.W. Smith
Dartmouth College

To a large extent, computing systems are useful only to the degree in which they're embedded in the processes that constitute human society. This embedding makes effective system security extremely important, but achieving it requires a strong look at the human side of the picture—the computers themselves are only part of the system.

IEEE Security & Privacy has covered these topics in the past, but usually from the perspective of computing, not society. Can we make it easier for human users to correctly trust what their computers are telling them? Can we make it easier for human programmers to write code that achieves desired functional and performance goals, but with fewer vulnerabilities?

Motivated by a series of events over this past year, we'll look at the societal aspects in this installment: the formal education process through which we train students, young and old, to be effective cyber-citizens; and the media coverage and editorializing process through which we express (or perhaps imprint) ethical judgment.

Pretend security for Web sites

Let's begin with the infamous business-school-applicant cases from earlier this year.[1,2] Several business schools, including those at Harvard, Stanford, and Dartmouth, outsourced online handling of applications to the recruiting firm Apply Yourself. Each applicant could create an online account, and then establish authenticated sessions to submit and access their application information. One such piece of information was whether the applicant had been accepted.

In the intended functionality, business schools would contact applicants on decision day and tell them how to learn their fate via the ApplyYourself portal. However, some schools posted the information early, and some students figured out which URL would give them access. The consequence was righteous indignation. Editorial writers and college students (as well as many of my professional colleagues) characterized these actions as "hacking" and denounced these applicants as embodying the same unethical mindset responsible for the Enron debacle and similar social ills. Most of the business schools summarily denied admission to these so-called hackers. (I'm proud to say that Dartmouth, my employer, was one of the few schools that didn't.)

This indignation troubles me because it overlooks several important facts. First, editing a URL doesn't constitute hacking. As any scholar in this information age knows, it has become standard behavior for literature searches: "Google took me to this interesting paper in an online proceedings—can I find the table of contents for the whole set?" Second, these applicants accessed their own information only; before entering the URL, they had to authenticate themselves. Third, the applicants received this information because the server gave it to them. Some editorial writers used the metaphor that students snuck into an unlocked office and examined a filing cabinet. A better metaphor would be that students were explicitly told that the doorman outside would answer their questions, and some of them asked him early. It would have been simple to instruct the doorman to not answer questions until the appropriate day, but no one thought to do that, and no one seems to have any moral indignation for the parties who were actually responsible for the privacy spill.

Ultimately, responsible citizenship—not to mention effective business leadership—requires perceiving and acting on what the technology really does, rather than putting blinders on and adhering to a collective fantasy of what some would like it to. I would be worried if leaders in business—or any other arena—didn't have an honest understanding of what their technology did and didn't do, and how secure it was against what kinds of adversaries, even ordinary users engaged in ordinary behavior. Unfortunately, this business-school incident seems to have established a worrying precedent: future leaders who understand the technology will be punished. Continuing to pretend the emperor has nice clothes won't help the emperor or produce more effective tailors.

Missing outrage

Although the business-school incident at Harvard received international attention, the media paid very little notice to an article in the 21 January 2005 edition of *The Harvard Crimson*.[3,4] It reported that Harvard insurer PharmaCare had set up a Web site that supplied a student's pharmaceutical records to anyone who could provide the student's birthday and Harvard ID number—both of which are publicly available. Clearly, disclosing information such as "student X has prescriptions for antidepressants" could have far more serious and irreversible consequences than "you were admitted to business school," so where was the outrage? Why did none of the voices calling for the business-school applicants to be tarred and feathered call for harsher punishment for the IT managers who committed a far worse offense—or the admissions IT people who didn't learn from it?

As the year wore on, more incidents seemed to fit the business-school pattern: the technology deployers becoming irate that their fantasies of security were disrupted, and media and popular opinion playing along.

Pretend security for WLANs

The 4th of July—a date typically associated with freedom in this country—brought a disturbing example: a man in Tampa Bay, Florida, was charged with a third-degree felony for "hacking" into an open WLAN.[5]

Home and enterprise networking is shifting from tethered to wireless, fundamentally changing the access paradigm because the network access world no longer directly corresponds to the physical access world. With tethered networking, a user needs an Ethernet jack to get on the local network. In the past, restrictions such as walls and locked doors for keeping unauthorized users out of buildings and rooms also kept them away from the jacks. However, wireless is different. Anyone within range of the radios can join the network, and the radio doesn't necessarily respect the traditional boundaries of walls and locked doors. Furthermore, access points, in their typical out-of-the-box configurations, happily advertise themselves as open links, and client platforms happily find them. Countermeasures exist, ranging from the ambitiously named *wired equivalent privacy* (WEP), which is easily compromised with appropriate tools, to new *Wi-Fi protected access* (WPA), which can encapsulate a wide range of authentication techniques (some of which aren't easily spoofed).

Police and media characterize the Tampa Bay gentleman's actions as breaking and entering—the owner was "victimized." A more appropriate metaphor is the network owner chose to leave his Ethernet jacks on the public sidewalk. If he wanted them protected, turning on even weak WEP—the moral equivalent of a "no trespassing" bit—is trivial. In the circles I travel, using an open wireless network is as ethical as throwing some litter in a trashcan left out on the street. Indeed, many people deliberately leave wireless access points open as a quiet public service. I know at least one network expert who actually reprogrammed his neighbors' wireless access points to keep them from interfering with each other, thus providing better coverage for everyone. (However, I'm not sure how his action fits into the moral framework.)

Despite its generally alarmist tone, the article in *The St. Petersburg Times* at least noted the other side of the issue as well, and quoted columnist Randy Cohen observed that "the person who opened up access to you is unlikely even to know, let alone mind, that you've used it. If he does object, there's easy recourse: nearly all wireless setups offer password protection."[5] Nonetheless, some poor soul now faces felony charges.

Pretend security for laptops

Another example of applying real

punishment to violators of pretend security occurred at Kutztown High School (in Kutztown, Pennsylvania), which distributed laptops to 600 students in academic year 2004 to 2005. To keep students from using inappropriate applications or visiting unsuitable Web sites, the school district installed restrictions on the machines and protected them with an administrator password. Some of the students found a way to subvert these restrictions, and after repeated failed attempts to stop this practice, the school district lodged criminal charges against 13 students for felony criminal trespass.[6]

How did these students subvert the restrictions? Did they hack it with buffer-overflow tools, or bootable USB flash drives? Nope: the administrative password was taped to the bottom of each laptop! (Adding insult to injury, the password itself was an easy derivation of the school's address.)

Writers have pointed out additional complexities in the case,[7,8] and the felony charges were dropped in exchange for an apology and some community service,[9] but the basic facts remain: the school district gave students laptops with the administrator password taped to them, the students used that password, yet the students were charged with felonies.

Pretend security education and training

What are we teaching the next generation of IT users, designers, and managers—as well as those who will write and enforce the laws governing this technology? We should teach them that IT will continue to permeate and change society in ways we can barely imagine, and how they need to be ready for it. We should teach them that effective security techniques require careful consideration of many factors, such as reasonable use and barriers. We should also teach them that security for an IT service deserves the same basic good sense and civic responsibility that fire safety and food purity receive, particularly when the consequences of compromise might be serious.

Unfortunately, we seem to be teaching them that it's acceptable to deploy slipshod protections—and then pillory those who realize this. We teach them it's wrong to disrupt the fantasy that the system works as the deployer imagines it, rather than as it actually does.

I certainly believe in rules of fair play and good sportsmanship. As an undergrad and as a professor, I've attended institutions with an "honor code"—students have easy opportunity to cheat but pledge not to. For the most part, I've found that they don't. When I teach security material, I explicitly tie student acquisition of this knowledge to the honor code. If the business-school applicants were told "we expect you not to look for your decision before day Y," or the Kutztown high-school students were told "we expect you not to visit these types of sites or download these types of applications," only then should punishment be doled out. However, this punishment should be for violating a social agreement, not for "breaking" security. If the drive-by networker in Florida had used Kismac to crack a WEP key or had reprogrammed his wireless card to have a blessed MAC, then he deliberately jimmied a lock open or walked by a clearly posted "no trespassing" sign.

My friend Gene Spafford, of Purdue, once characterized defenders of Robert Morris (of Morris Worm fame) as "blaming an arson victim for the fire because she didn't build her house of fireproof metal,"[10] but I see this current situation as more akin to building a house so fragile that knocking on the door causes it to fall down—and then arresting the visitors who knock on the door. Like it or not, knocking on a door—like connecting to an open wireless network or editing URLs—is ordinary behavior. One colleague asked whether I'm making an "ease of attack" argument, akin to those people who would never steal a music CD from a store, but have no compunction against downloading pirated MP3s. My answer is no: in that case, the music's owner isn't the one making it easy to download the file. In the other cases, though, the "victimized" owner could have easily set up barriers against what is otherwise acceptable usage, but for some reason chose not to. If we as a society are going to build technology that matches acceptable norms of usage, we need to honestly evaluate what it does, rather than basing policy, law, and social convention on what some would like to pretend that it does.

Fortunately, there are glimmers of hope. Vermont Technical College, for example, recently discovered a large privacy spill—student records were readily available on the open Internet for "more than 18 months." An alum who was Googling his own name discovered the spill. Did VTC bring charges against him, or did the press vilify him for hacking? Refreshingly, no: VTC responded by reviewing its information security practices and adding more security training.[11]

The emerging information age presents us with numerous challenging scenarios in which we need to think carefully about what's right and wrong, what constitutes reasonable and prudent behavior, and what we can do with technology to make it easier for the right things to happen. Evaluating these decisions requires clear-headed thought and sensible discussion. The continued trend of histrionics with each new incident takes us in exactly the

Suggestions welcome

If you have a timely or interesting idea that you think I should cover in this department, or if you would like to contribute a piece, please email me at sws@cs.dartmouth.edu.

wrong direction. Fuss and indignation—and demonization of those with the best grasp of the technology in question—won't prepare us for a secure future. If there had been a Digital Millennium Copyright Act for the automobile industry, Ralph Nader would have spent his career in prison, and we'd all still be driving—and dying in—Corvairs. ▢

References

1. E. Felten, "Harvard Business School Boots 119 Applicants for 'Hacking' into Admissions Site," *Freedom to Tinker*, 9 Mar. 2005; www.freedom-to-tinker.com/?p=780.
2. "HBS/ApplyYourself Admit Status Snafu?" *Poweryogi*, 2 Mar. 2005; http://poweryogi.blogspot.com/2005/03/hbsapplyyourself-admit-status-snafu.html.
3. J.H. Russell and E.S. Theodore, "Drug Records, Confidential Data Vulnerable," *The Harvard Crimson*, 21 Jan. 2005; www.thecrimson.com/article.aspx?ref=505402.
4. J. Russell, "Harvard Fixing Data Security Breaches Loophole Allowed Viewing Student Prescription Orders," *Boston Globe*, 22 Jan. 2005; www.boston.com/news/local/massachusetts/articles/2005/01/22/harvard_fixing_data_security_breaches/.
5. A. Leary, "Wi-Fi Cloaks a New Breed of Intruder," *St. Petersburg Times*, 4 July 2005; www.sptimes.com/2005/07/04/State/Wi_Fi_cloaks_a_new_br.shtml.
6. "Felony Charges for Computer-Abusing Kids," *eSchool News Online*, 11 Aug. 2005; www.eschoolnews.com/news/showStory.cfm?ArticleID=5820.
7. B. Schneier, "The Kutztown 13," *Schneier on Security*, 22 Aug. 2005; www.schneier.com/blog/archives/2005/08/computer_crime.html.
8. A. Kantor, "Kutztown Kids Aren't the Good Guys," *USA Today*, 18 Aug. 2005; www.usatoday.com/tech/columnist/andrewkantor/2005-08-18-kutztown-kids_x.htm.
9. "'Kutztown 13' Hackers Quietly Offered Deal," *eSchool News Online*, 30 Aug. 2005; www.eschoolnews.com/news/showStory.cfm?ArticleID=5891.
10. E. Spafford, "The Internet Worm: Crisis and Aftermath," *Comm. ACM*, vol. 32, no. 6, 1989, pp. 678–687.
11. J. Fahy, "Vt. Tech Exposes Students' Data," *The Burlington Free Press*, 20 Oct. 2005, p. 01b.

***S.W. Smith** is an assistant professor at Dartmouth College; he previously worked as a research scientist at IBM Watson and at Los Alamos National Lab. His research interests include trusted computing, public-key infrastructures, and human-computer interaction aspects of security (HCISEC). Smith has a PhD in computer science from Carnegie Mellon University. Contact him at sws@cs.dartmouth.edu.*

ADVERTISER / PRODUCT INDEX NOVEMBER/DECEMBER 2005

Advertiser	Page Number
Charles River Media	**11**
Hindawi Publishing Corp.	**5**
ISSSE 2006	**Cover 3**
RSA Conference 2006	**Cover 4**

Boldface denotes advertisements in this issue.

Advertising Personnel

Marion Delaney
IEEE Media, Advertising Director
Phone: +1 212 419 7766
Fax: +1 212 419 7589
Email: md.ieeemedia@ieee.org

Marian Anderson
Advertising Coordinator
Phone: +1 714 821 8380
Fax: +1 714 821 4010
Email: manderson@computer.org

Sandy Brown
IEEE Computer Society,
Business Development Manager
Phone: +1 714 821 8380
Fax: +1 714 821 4010
Email: sb.ieeemedia@ieee.org

Advertising Sales Representatives

Mid Atlantic (product/recruitment)
Dawn Becker
Phone: +1 732 772 0160
Fax: +1 732 772 0161
Email: db.ieeemedia@ieee.org

New England (product)
Jody Estabrook
Phone: +1 978 244 0192
Fax: +1 978 244 0103
Email: je.ieeemedia@ieee.org

New England (recruitment)
John Restchack
Phone: +1 212 419 7578
Fax: +1 212 419 7589
Email: j.restchack@ieee.org

Connecticut (product)
Stan Greenfield
Phone: +1 203 938 2418
Fax: +1 203 938 3211
Email: greenco@optonline.net

Midwest (product)
Dave Jones
Phone: +1 708 442 5633
Fax: +1 708 442 7620
Email: dj.ieeemedia@ieee.org
Will Hamilton
Phone: +1 269 381 2156
Fax: +1 269 381 2556
Email: wh.ieeemedia@ieee.org
Joe DiNardo
Phone: +1 440 248 2456
Fax: +1 440 248 2594
Email: jd.ieeemedia@ieee.org

Southeast (recruitment)
Thomas M. Flynn
Phone: +1 770 645 2944
Fax: +1 770 993 4423
Email: flynntom@mindspring.com

Southeast (product)
Bill Holland
Phone: +1 770 435 6549
Fax: +1 770 435 0243
Email: hollandwfh@yahoo.com

Midwest/Southwest (recruitment)
Darcy Giovingo
Phone: +1 847 498-4520
Fax: +1 847 498-5911
Email: dg.ieeemedia@ieee.org

Southwest (product)
Josh Mayer
Phone: +1 972 423 5507
Fax: +1 972 423 6858
Email: jm.ieeemedia@ieee.org

Northwest (product)
Peter D. Scott
Phone: +1 415 421-7950
Fax: +1 415 398-4156
Email: peterd@pscottassoc.com

Southern CA (product)
Marshall Rubin
Phone: +1 818 888 2407
Fax: +1 818 888 4907
Email: mr.ieeemedia@ieee.org

Northwest/Southern CA (recruitment)
Tim Matteson
Phone: +1 310 836 4064
Fax: +1 310 836 4067
Email: tm.ieeemedia@ieee.org

Japan
Tim Matteson
Phone: +1 310 836 4064
Fax: +1 310 836 4067
Email: tm.ieeemedia@ieee.org

Europe (product)
Hilary Turnbull
Phone: +44 1875 825700
Fax: +44 1875 825701
Email: impress@impressmedia.com