By GREGORY CONTI, *Guest Editor*

HACKING AND INNOVATION

Why computer science should pay serious attention to the hacking community and its passion for pushing the limits of technology and its role as a counterbalance to its misuse.

There is a passionate and independent-minded global community of highly skilled technical experts that frequently functions outside the mainstream of computer product development and conventional technology research. Sometimes called the hacker community, these experts are responsible for innovation that pushes the limits of technology, sometimes in unintended or uncomfortable ways, as well as for prescient warnings about the threats of both technology and the government's technology-related policy and regulations. Computer scientists have much to learn about innovation and nontraditional problem solving by listening to and working with them.

ILLUSTRATION BY JEAN-FRANÇOIS PODEVIN

MY AIM IS TO CLOSE THE GAP
BETWEEN THE COMMUNITIES OF COMPUTER PROFESSIONALS AND COMPUTER HACKING.

Whether inside or outside the mainstream, hackers are less constrained by conventional thinking, and their work often complements (and sometimes conflicts with) its counterpart in traditional industrial organizations, academic departments, and government agencies. In many cases their research is ahead of what's being done in these organizations but with results that are unlikely to ever appear in academic journals and conferences due to differing ways of disseminating information.

Their passion is especially noteworthy. From Nguyen Phuoc Huy, a medical doctor from the Mekong Delta region of Vietnam who built his own endoscope out of a low-cost Web camera [5], to the Shmoo collective's Wired Equivalent Privacy (WEP)-cracking robot (see Figure 1), to Ward Christensen's and Randy Suess's construction of the first electronic bulletin board system (see Figure 2) in 1978, the contributions are diverse and significant.

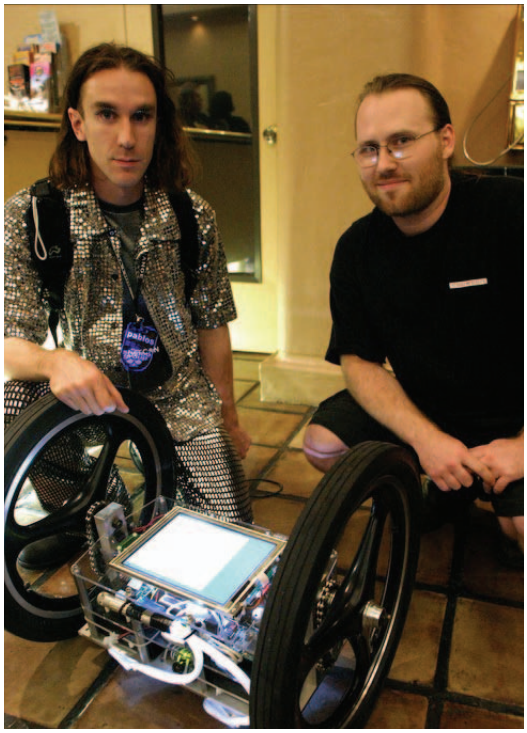

Figure 1. The Shmoo collective's WEP-cracking robot (photograph by Declan McCullagh, www.mccullagh.org).

Some computer scientists consider it a high honor to be described as a hacker; to others it's a base insult. For many computer scientists, as well as the general public, the word hacker has a connotation reflecting the sensationalized stereotype often seen in mainstream media. Objective accounts are rare [1–4]. Perhaps due to this perception, two disjoint, typically mistrustful, technology-focused communities—professional computing and hacking—have emerged. Despite having only infrequent interactions, they are often at odds, ultimately frustrating one another's efforts. As the world increasingly depends on technology, we all must move beyond the semantics and etymology of the word hacker [6] to address the true risks and needs of humanity, either through our own research or when we serve as technical advisors to legislative and technology policy decision makers. Ultimately, each of our scientific contributions should be weighed on the merit of the related ideas, not on academic credentials, institutional affiliation, or age of the source.

Our goal here is to listen to the authentic and expert voice of hacking—a task more difficult than it might appear. The loose-knit hacker community has no formal leaders. Hacking is diverse and by its nature resists formal definition. We have sought out a sample from among the best and the brightest. To this end, these articles were written by individuals who routinely challenge convention, whether from inside the professional computing community or from within the computer underground. Many have never published in the scientific literature before. This fact does not, however, diminish the value of their words but should instead make us listen even more attentively.

The hacker community possesses an extensive body of work, but instead of lying in repositories (such as ACM and IEEE digital libraries), results are presented at such conferences as Black Hat, CanSecWest, the Chaos Computer Congress, DEF CON, HOPE, Interz0ne, ShmooCon, and Toorcon or published in such magazines as *2600, BinRev,* and *Phrack* (see the sidebar "Hacking Sources"). The fact that the ideas exist in circles less traveled by the academic community does not relieve us of the responsibility of exploring them to research related work. You may be surprised to find that your "new" idea was promulgated years ago at a hacker conference or in a

hacker publication. Almost without exception, these articles, presentations, and other artifacts are freely available online.

I have been profoundly influenced by Orson Scott Card's portrayal of youthful prodigies in his 1985 science fiction novel *Ender's Game* in which Ender's siblings, Peter and Valentine, were prodigies too young, despite their great intelligence, to be accepted by the great thinkers and leaders of their day. Despite this impediment, they nevertheless rose to prominence on the merit of their ideas alone by using anonymous online personas to promulgate their thoughts. Similarly, when seeking appropriate and authentic voices for this section, I sought out deep thinkers and gifted technical experts, who, through the power of their words alone, could describe serious personal experience and insights so compelling that virtually any reader from either community would acknowledge the value of their message, even if that reader does not fully agree. My aim is to close the gap between the communities of computer professionals and computer hacking.

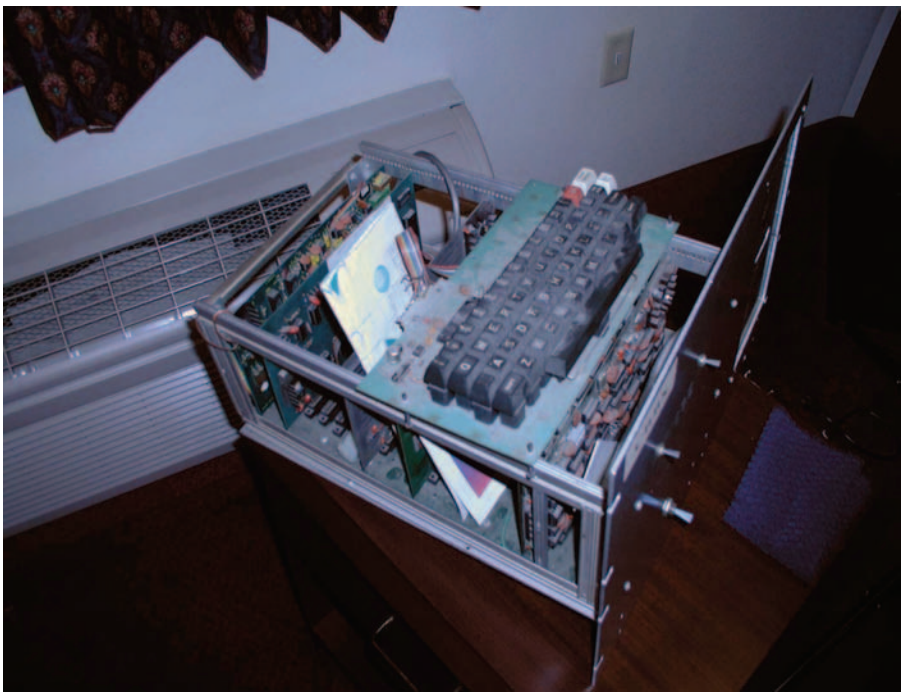

Figure 2. The first electronic bulletin board system (1978) built by Ward Christensen (software) and Randy Seuss (hardware), both members of the Chicago Area Computer Hobbyists' Exchange (photograph by Jason Scott, www.bbsdocumentary.com).

The section has two main components: personal viewpoints and in-depth technical articles. I challenged the viewpoint authors to discuss some of the most significant trends and threats they saw emerging in the worldwide Internet-based environment. Tom Cross, creator of the MemeStreams semantic blogging system, which helps people share information about what's worth reading on the Web, starts us off by exploring the troubling decline in the right of individual experimenters to freely investigate technology. Steve Bono et al. then address the use of the courts, legislation, and government regulation to prevent discourse about vulnerabilities in software and hardware products.

I challenged the technical article writers to explore three facets of hacking—software, hardware, and networks—and explain their personal methods and thought processes when approaching problems. Joe Grand peels back the covers on hardware to reveal approaches to modifying technology in ways unintended by its designers. Bruce Potter, founder of the Shmoo Group of security professionals, well-known for its annual security conference Shmoocon, describes how wireless hotspots break down the traditional security trust model, leaving the typical end user, as well as many power users and even many global corporations, underprotected from potential malicious attack.

Felix "FX" Lindner examines the similarity of the software engineering and security disciplines, finding that, despite that similarity, different approaches and terminology result in less-secure systems. Finally, Dan Kaminsky explores key aspects of request for comment-compliant Domain Name System (DNS) protocol hacking, by probing DNS servers worldwide in order to notify DNS operators of their vulnerabilities. He also shares his work mapping the global spread of the recent Sony rootkit that put a visible face on the magnitude and location of those infected, helping raise a public outcry against Sony's intrusion.

Hacking is more about innovation and less about computer security. Hacking and computer science are so intertwined it is a travesty the two communities do not share greater respect for and cooperation with one another. To promote the sharing of common interests the hacking story must be told accurately in all its sometimes contradictory aspects. *Communications*

represents the public record for the professional computer science community. This section is our attempt to add to this record a glimpse of the heart and soul of the hacker ethic in its members' own words.

There is a narrow path for success that will help foster collaboration between the two sides of the divide. Antagonists and critics from both sides are waiting to pounce, but the potential for success makes the risk worthwhile. To move beyond common stereotypes, we may work together to advance the interests of human knowledge. The main message we hope to impart is that you should feel free to challenge convention, explore the work done by these researchers, and seek opportunities to collaborate with the hacking community. I ask that you suspend your preconceived notions, ponder the arguments and expertise, and, perhaps, adjust your personal perspective. I daresay you will be more warmly received in their world than they would in ours. Perhaps we can change that. C

The views expressed here are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense, or the U.S. Government.

References

1. Caloyannides, M. Enhancing security: Not for the conformist. *IEEE Security and Privacy 2,* 6 (Nov./Dec. 2004).
2. Conti, G. Why computer scientists should attend hacker conferences. *Commun. ACM 48,* 3 (Mar. 2005), 23–24.
3. Cowan, C., Arnold, S., Beattie, S., Wright, C., and Viega, J. Defcon capture the flag: Defending vulnerable code from intense attack. In *Proceedings of DARPA DISCEX III* (Washington, D.C., Apr. 22–24). IEEE Computer Society Press, Los Alamitos, CA, 2003.
4. Graham, P. *The Word Hacker*. Posted on a personal Web site. (Apr. 2004); www.paulgraham.com/gba.html.
5. Le, H. Vietnam medic makes DIY endoscope. BBC News Online (Aug. 22 2005); news.bbc.co.uk/1/hi/technology/4145984.stm.
6. Raymond, E. The Jargon File 4.4.7. (Dec. 29, 2003); www.catb.org/~esr/jargon/html/H/hacker.html.

Gregory Conti (conti@acm.org) is an Academy Professor of Computer Science at the United States Military Academy, West Point, NY, and currently at the Georgia Institute of Technology, Atlanta, on a Department of Defense Fellowship.

HACKING SOURCES

The following sources of information are a great starting point for learning about the hacking community:

Conferences

Blackhat (Las Vegas, NV)
www.blackhat.com

CanSecWest (Vancouver, British Columbia)
www.cansecwest.com

Chaos Computer Congress (Berlin, Germany)
www.ccc.de

DEFCON (Las Vegas, NV)
www.defcon.org

Hack.lu (Luxembourg/Kirchberg)
www.hack.lu

Interzone (Atlanta, GA)
www.interzone.com

PACSEC (Tokyo)
www.pacsec.jp

RECON (Montreal, Canada)
www.recon.cx

RuxCon (Sydney, Australia)
www.ruxcon.org.au

Shmoocon (Washington, D.C.)
www.shmoocon.org

ToorCon (San Diego, CA)
www.toorcon.org

What the Hack (Den Boesch, The Netherlands)
www.whatthehack.org

Magazines and Journals

2600 Magazine
www.2600.com

BinRev
www.binrev.com

Hacker Japan
www.byakuya-shobo.co.jp/hj

Make Magazine
www.makezine.com

Phrack
www.phrack.org

Books

Hackers and Painters (2004) by Paul Graham

Silence on the Wire by (2005) Michal Zalewski

Video

BBS Documentary
www.bbsdocumentary.com

Regularly Scheduled Meetings (open to all)

2600 Meetings
www.2600.com/meetings

Defcon Groups
www.defcon.org/html/defcon-groups/dc-groups-index.html