CROSSTALK

Sponsor *Lt. Col. Joe Jarzombek*
801-777-2435 DSN 777-2435
jarzombj@software.hill.af.mil

Publisher *Reuel S. Alder*
801-777-2550 DSN 777-2550
publisher@stsc1.hill.af.mil

Managing Editor *Forrest Brown*
801-777-9239 DSN 777-9239
managing_editor@stsc1.hill.af.mil

Senior Editor *Sandi Gaskin*
801-777-9722 DSN 777-9722
senior_editor@stsc1.hill.af.mil

Graphics and Design *Kent Hepworth*
801-775-5798
graphics@stsc1.hill.af.mil

Associate Editor *Lorin J. May*
801-775-5799
backtalk@stsc1.hill.af.mil

Editorial Assistant *Bonnie May*
801-777-8045
editorial_assistant@stsc1.hill.af.mil

Features Coordinator *Denise Sagel*
801-775-5555
features@stsc1.hill.af.mil

Customer Service 801-775-5555
custserv@software.hill.af.mil

Fax 801-777-8069 DSN 777-8069

STSC On-Line http://www.stsc.hill.af.mil

CROSSTALK On-Line http://www.stsc.hill.af.mil/Crosstalk/crostalk.html

ESIP On-Line http://www.esip.hill.af.mil

Subscriptions: Send correspondence concerning subscriptions and changes of address to the following address:

Ogden ALC/TISE
7278 Fourth Street
Hill AFB, UT 84056-5205

E-mail: custserv@software.hill.af.mil
Voice: 801-775-5555
Fax: 801-777-8069 DSN 777-8069

Editorial Matters: Correspondence concerning *Letters to the Editor* or other editorial matters should be sent to the same address listed above to the attention of *CROSSTALK Editor* or send directly to the senior editor via the E-mail address also listed above.

Article Submissions: We welcome articles of interest to the defense software community. Articles must be approved by the *CROSSTALK* editorial board prior to publication. Please follow the *Guidelines for CROSSTALK Authors*, available upon request. We do not pay for submissions. Articles published in *CROSSTALK* remain the property of the authors and may be submitted to other publications.

Reprints and Permissions: Requests for reprints must be requested from the author or the copyright holder. Please coordinate your request with *CROSSTALK*.

Trademarks and Endorsements: All product names referenced in this issue are trademarks of their companies. The mention of a product or business in *CROSSTALK* does not constitute an endorsement by the Software Technology Support Center (STSC), the Department of Defense, or any other government agency. The opinions expressed represent the viewpoints of the authors and are not necessarily those of the Department of Defense.

Coming Events: We often list conferences, seminars, symposiums, etc., that are of interest to our readers. There is no fee for this service, but we must receive the information at least 90 days before registration. Send an announcement to the *CROSSTALK* Editorial Department.

STSC On-Line Services: STSC On-Line Services can be reached on the Internet. World Wide Web access is at http://www.stsc.hill.af.mil. Call 801-777-7026 or DSN 777-7026 for assistance, or E-mail to schreifr@software.hill.af.mil.

Publications Available: The STSC provides various publications at no charge to the defense software community. Fill out the Request for STSC Services card in the center of this issue and mail or fax it to us. If the card is missing, call Customer Service at the numbers shown above, and we will send you a form or take your request by phone. The STSC sometimes has extra paper copies of back issues of *CROSSTALK* free of charge. If you would like a copy of the printed edition of this or another issue of *CROSSTALK*, or would like to subscribe, please contact the customer service address listed above.

The ***Software Technology Support Center*** was established at Ogden Air Logistics Center (AFMC) by Headquarters U.S. Air Force to help Air Force software organizations identify, evaluate, and adopt technologies that will improve the quality of their software products, their efficiency in producing them, and their ability to accurately predict the cost and schedule of their delivery. *CROSSTALK* is assembled, printed, and distributed by the Defense Automated Printing Service, Hill AFB, UT 84056. *CROSSTALK* is distributed without charge to individuals actively involved in the defense software development process.

The New Terrorists

If you're having problems with snakes coming to get you from behind your bedroom chair at night, it helps to turn up the lights, open the door a crack, and squeeze the stuffing out of your Tickle-Me-Ernie doll. Just ask my two-year-old son, Daren. He still doesn't know where his dreams stop and reality begins, but he feels much safer since we instituted these powerful anti-snake defenses.

Thankfully, unlike toddlers, we adults can separate fantasy from reality. For example, a few years ago, a movie about computer cracking and sabotage called "*The Net*" came out. It was packed with eye rollers, but these were quickly re-butted by Internet chat forums in one huge collective "Puh-LEEZE!"

The first clue about the movie's realism was that the lead character, a lonely geek beta tester, was played by the lovely Sandra Bullock—a casting decision equivalent to making a movie about the Miss America Pageant with the lead, Miss Delaware, played by Wilford Brimley. (Not that the cyberculture—which likely includes readers of this journal—isn't full of attractive, fascinating people who are neither sensitive to negative stereotypes nor vindictive toward those who propagate these stereotypes. Ha-ha! Please leave my medical records alone!)

However, it was mostly the technical issues that made net surfers guffaw at "*The Net.*" For example, Bullock's character routinely accesses an advanced multimedia Internet full of cutesy features unavailable to the general public at approximately 1,153 times the bandwidth of typical modems. And get this: The bad guys manage to steal vast sums and even kill people by breaking into critical banking, police, hospital, and air-traffic computers.

Ha-ha! *Hacker terrorists?* What planet do these Hollywood types live on, where critical computer systems are even indirectly connected to the Internet, opening the door for terrorist geeks to remotely break in and cause havoc?

Well, okay, the world is spending billions of dollars each year to allow exactly that. That's why I wanted to see if cyberterroism were for real or just a hyped-up Hollywood dream. What I saw made my head spin like an unbalanced Maytag.

After a few clicks in *Yahoo!* I was visiting sites with step-by-step instructions on how to slip past firewalls, steal passwords, tap into phone and data lines, and cover your tracks. Plus, there were various free "cracking" tools available for download. Purveyors of this information seemed proud of the ease with which they allegedly find weak links and holes in supposedly secure systems, where they could cause serious damage if they were criminally inclined. (Which, of course, they never are! Please don't double my bank account balance!)

Speaking of which, I also read news reports on several successful electronic bank break-ins, including a partially successful $10 million heist. And according to the head of a major U.S. media organization, a team of hired government crackers last year showed what kind of damage organized terrorists could do. Using only techniques found on the Internet, they allegedly broke into "secure" computers and made power grids fail, air traffic control systems go haywire, oil refinery pumps stop working, and they compromised supply networks. They supposedly covered their tracks well enough that the victims wouldn't acknowledge being cracked—these were considered unexplainable glitches, not attacks.

So as we blithely barge headlong into a world where every critical computer system is in some way connected to the Internet—I suppose someone is already working on a method to remotely pilot oil tankers over the Web—I wonder how often we're stopping to ask the following questions.

- Just because a system *can* have a Web interface, does that mean it *should*?
- If a critical systems is accessible to anyone with a Web browser and password, why do crackers snicker so loudly when such a system is declared "secure"?
- Could evil crackers rig it so that the Miss America Pageant was actually won by Wilford Brimley? Would this help resolve the swimsuit debate?

These tough questions impact all of us. And the fuzzy line between fact and fiction makes me wonder: How real and dangerous are terrorist "cybersnakes"? Are our defenses good or are we counting on "Ernie" to protect us? We must address these questions, or later we may have tougher questions to answer. For example: mascara or no mascara for Miss Delaware's back hair? – Lorin May

Got an idea for BACKTALK? Send an E-mail to backtalk@stsc1.hill.af.mil