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-M e-Ernie doll. Just ask my two-year-old son, D aren. 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 Nxt” came out. It was packed with eye rollers, but these were quickly rebutted by Internet chat forums in one huge collective “Puh-LEAN!”

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. H ah ha! Please leave my medical records alone!)

However, it was mostly the technical issues that made net surfers guffaw at “The Nxt.” For example, Bullock’s character routinely accesses an advanced multimedia Internet full of cutey 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.

H a 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 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 cyberterrorism 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 track your covers. 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. (W hich, 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 M ay

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