Changing the Puzzle Pieces

Carl E. Landwehr
Associate Editor in chief

You might remember the American remake of the British movie *Bedazzled* released a few years ago. It featured an office geek who sells his soul to the devil for seven wishes. His first wish? To be rich, powerful, and married to his dream girl. The devil fulfills all those wishes at once—by turning him into a Columbian drug lord.

Many fairy tales embed the notion of people wishing for something only to be dismayed when they get it. For the past several decades, we technologists seem to have been getting our wishes in a big way. For a recent talk, I Googled for numbers and found that the retail price of disk storage for PCs has dropped about five decimal orders of magnitude (DOMs) in 25 years. The number of transistors per chip has grown about 5.5 DOMs in the same period, while processor clock rates increased two DOMs in about 15 years. From 1990 to 2002, Internet traffic grew more than five DOMs, and the number of IP addresses with assigned names grew about two DOMs. These changes are huge—indeed, magical.

At the same time, the plague of spam, spyware, viruses, and worms saps the network and computing capacity actually available to us. I have seen estimates that as much as 90 percent of the email arriving at AOL's doorstep today is spam. CERT incident reports grew five DOMs in 15 years—to such a point that CERT no longer reports this number because, "given the widespread use of automated attack tools, attacks against Internet-connected systems have become so commonplace that counts of the number of incidents reported provide little information with regard to assessing the scope and impact of attacks" (www.cert.org/stats/#incidents).

Another measure of the problem is the speed with which attacks propagate: the excellent visualizations prepared by the Cooperative Association for Internet Data Analysis (CAIDA, www.caida.org) show CodeRed's worldwide spread in July 2001—300,000 hosts infected in less than a day—and the startlingly fast spread of the SQL Slammer worm in 2003: 75,000 hosts in less than a half-hour.

It is as if we wished for processing, storage, and communications, but forgot to mention security or dependability. Of course, these changes didn't happen magically or through some Faustian bargain. We invented, developed, marketed, and purchased the technologies with which we are now both blessed and cursed. We create puzzles for ourselves—but can we solve them?

As Cyber Trust program director at the US National Science Foundation, I see many researchers' wishes in the form of grant proposals, only a small fraction of which NSF is able to fulfill. In 2004, Cyber Trust received 390 proposed research projects, of which only 35 could be funded. NSF employs careful procedures for peer-reviewing proposals, of course, but the outcomes are still hard to predict because NSF strives to fund the best ideas offered, regardless of the directions they might take. (See www.nsf.gov for details on Cyber Trust awards.)

The DOM advances in other technologies have been fueled by a combination of research investment and market forces, stimulating both new knowledge and commercial innovation. Can these same forces improve security as well? In the preface to her recently released book, *The Economics of Computer Security* (Kluwer, 2004), Jean Camp of the University of Indiana argues that the computer security market has failed. But new security products are continually coming to market, and AOL's recent decision to make secure identification tokens available to its users seems a positive indication of increasing market interest in security.

On the research side, NSF's investments in basic cybersecurity research over the past few years have risen, but it's difficult to gauge research investments comprehensively. There is evidence of growing interest in cybersecurity research internationally as well, in both Europe and Asia. A subcommittee of the President's Information Technology Advisory Committee (PITAC) is currently studying federal cybersecurity research investment levels in the US and, by the

time you read this, might even have made its recommendations (see www.itrd.gov/pitac).

Could increases in cybersecurity research investments, combined with commercial uptake, lead us to a more trustworthy cyberinfrastructure? I believe so, but we must raise our sights. We don't *have* to live in a world where patches and worms chase each other around the networks on which we depend. The assumptions made by Internet protocol designers 20 and 30 years ago must change. If we must give up some assumptions, develop new protocols, and invent new devices, let's do it now. We built this puzzle, so we should remind ourselves occasionally that it's in our power to reshape the pieces. ▢

Interface

Letters to the Editor

Suggestions

Dear Editors,

I just wanted to congratulate you on keeping up the IEEE tradition of producing the best journals in its field. The latest issue of *IEEE Security & Privacy* has no less than three articles that I'll be forwarding on to my colleagues.

I have a couple of suggestions to improve the magazine even further. First, you might recommend to authors that they mention the tools they use to perform the security tasks they discuss in their articles. For example, structured risk analysis is a focus of my work, but I wasn't familiar with the Morda technique the authors discussed in "Risk-Based Systems Security Engineering: Stopping Attacks with Intention" (On the Horizon, vol. 2, no. 6, 2004, pp. 59–62). The article contained some impressive graphics, but it wasn't clear whether they were produced by a defined Morda toolkit or whether they were developed ad hoc for this particular article.

Second, I subscribe to the electronic version of the magazine from the Digital Library, and the hyperlinked table of contents makes a vast difference in the ease of navigating around in it. In fact, electronic readers are likely to use the links exclusively. It might be worthwhile to expand the contents pages of electronic-edition magazines to include an entry to every page instead of continuing the tradition of leaving certain pages unindexed.

Still, in spite of the readability and portability advantages of ink-on-paper that are still about five times better than what we get from pixels-on-screen, its archival convenience and searching convenience make the electronic publication the equal of the hardcopy edition. If we ever get notebook displays that are readable in direct sunlight, I'll cancel even more of my hardcopy subscriptions.

Cheers,

George McKee,
IEEE Member

Thanks for your suggestion. The Digital Library team is currently working on enhanced and expanded linking functionality. —Eds.

Honeynets

Dear Editors,

I'm very disappointed about the statement at the end of the Honeynet Files: "The department has been discontinued to allocate additional space" (vol. 2, no. 6, 2004, pp. 73–75). Is the paper the problem or the lack of editorial staff?? I'm seriously considering canceling my subscription.

Kind regards,

Bruno Joho
IEEE Member

We hear you, as well as the voices of other readers who enjoy that department. On a regular basis, the Honeynet community will continue to contribute material about new exploits and trends to the Attack Trends department.

—Eds.

Erratum

In the November/December 2004 article, "Secure Real-Time Operating Systems at Lower Costs," by Benjamin Alfonsi, he mistakenly attributed a quote by Bob Morris, VP of LynuxWorks, to Roger Villareal of Weber Shandwick. Weber Shandwick is their PR agency (not a military RTOS vendor), and Villareal was speaking on behalf of Morris.

We regret the errors. *—Eds.*

Got comments? Log onto our community forum to post your views with your peers. Please visit us at www.ieeecommunities.org/securityandprivacy