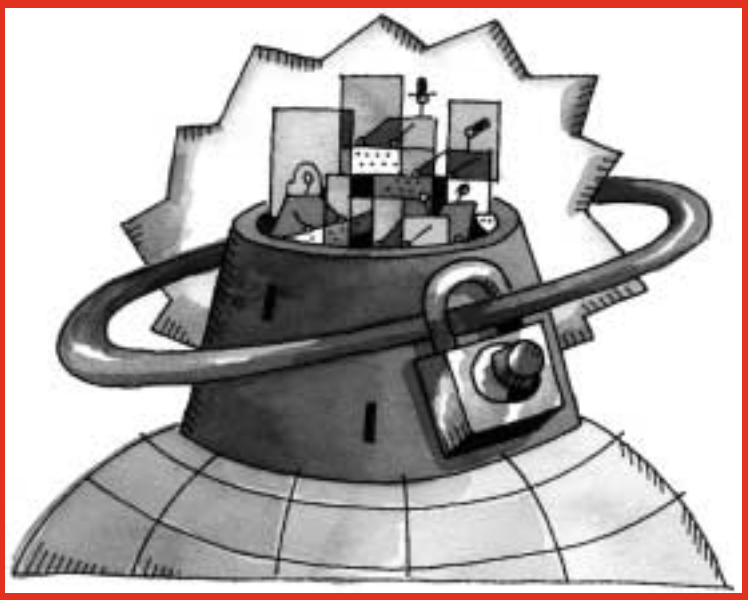
;login:
THE MAGAZINE OF USENIX & SAGE
December 2002 • volume 27 • number 6

Focus Issue: Security

Guest Editor: Rik Farrow

inside:



USENIX & SAGE
The Advanced Computing Systems Association &
The System Administrators Guild

in this issue

by Rik Farrow

Rik Farrow provides UNIX and Internet security consulting and training. He is the author of *UNIX System Security* and *System Administrator's Guide to System V*.

rik@spirit.com

I wanted to use an old photo to go with my comments for this, the fifth Security Special Edition of *;login:*. Why? This ID photo was taken in 1982, when I worked as a consultant for Morrow, an early designer and manufacturer of desktop computers. Morrow had brought in a security firm and had everyone get photo IDs, because they were losing a lot of money on stolen hard drives. In those days, a 34-megabyte hard drive cost nearly $2000 (when purchased in bulk) and had a high street value. Employees had been caught recovering hard drives from dumpsters – having previously put them into trash cans inside the building.

The addition of physical security made my life more difficult. I worked on two Morrow product lines, one that used CP/M and the other a version of UNIX. I had two hard drives, each with one OS on it, and would carry just the hard drives from my home office into Morrow. Getting administrative permission to do this was possible, but difficult.

My solution? Carry the hard drive in my backpack, under a spiral notebook. The guard would check my photo ID, look inside my backpack, which I would open wide for him. The heavy hard drive would sink beneath the notebook every time. So, to me, this old photo helps to remind me of the failings of security, even when it is as simple as a physical search.

At about the same time I was learning about UNIX by trying to teach other people about it; Tom Perrine was working with a group of people writing KSOS, a secure kernel designed to run under Version 6 UNIX. In his article, Perrine talks about how often today's programmers ignore lessons from the past. I did mention to Tom that the information that he wishes were better known used to be very secret. Many of us had copies of the Lion's notes (mine was at least 10th generation), which provided us with our *only* example of *any* operating system code or design. Things have gotten considerably better on this score, even if programmers are still working at re-inventing security.

Kevin Fu and his co-authors make the point that not everything about security was developed in the 1970s. Although they do leverage asymmetric encryption, a seventies invention, SFS provides true security but with a policy the opposite of most security policies: the remote users have control over their accounts, and anyone can decide to mount a public SFS share. SFS also incorporates other applications, including secure remote execution as an alternative to SSH and a read-only file system that uses digital signatures (making mirror sites much safer to use).

Jared Allison and George Jones, both from UUNET, provide practical discussions about taking advantage of logging and securing your network infrastructure, respectively. Two San Diego Supercomputing Center denizens wrote articles, one discussing computer legal practice (Erin Kenneally) and the other, how to start your own regional information watch (Abe Singer). Lance Spitzner, of the Honeynet Project, introduces HOSUS, a plan for getting early warnings about Internet attacks. And Sven Dietrich, of CERT, gets much more controversial with some of his suggestions for improving the security of Internet connected systems. And when it comes to the millions of poorly maintained Windows boxes attached to always-on connections these days, perhaps he has the right idea.

Ofir Arkin, of Sys-Security, presents us with just how insecure Voice over IP really is. Arkin has already come up with several advisories about vulnerabilities in different Internet phone products. Finally, Peter Salus describes his experiences during the Security Symposium.

This edition also includes the session summaries from the Security Symposium, something that I sincerely want to thank the summarizers for. One session did not get covered. A closing keynote had been scheduled, then a speaker substitution occurred, and then even the substitute flaked. Fortunately for USENIX, Dick Cheney was in town (San Francisco) to speak to some rich executives at a meeting in the Saint Francis Hotel. Not that Mr. Cheney wanted to speak to us, but his stand-in was more than willing.

The stand-in, a member of the San Francisco Mime Troupe (*http://www.sfmt.org*) lacked only a bevy of serious-looking Secret Service agents to complete the illusion. Ed Holmes gave a speech that, with the exception of several howlers, seemed just as authentic as any of the normal Administration double-speak. There were several people lined up to ask questions, starting with Peter Honeyman, who, for once, sounded to me completely inarticulate. John Gilmore, who has made a point of not traveling with photo ID, asked why he had to present ID to travel. The Cheney look-alike replied, "I don't have a problem traveling, what's wrong with you?" Holmes finished up by inducting the attendees into the Web Rangers, and enjoined them to report any "suspicious activities" they or their associates might be engaged in to the "government."

Some of what you will find in this issue comes from the hall talk – what goes on between sessions at any USENIX conference. But nothing can substitute for the experience and fun of actually being there.

One of the issues that I touched upon above, the millions of Internet-connected Windows systems, is likely to become an even more serious security problem over time. Today, the spread of worms and email viruses gets a lot of help from home systems. According to David Moore of CAIDA (at SDSC), Code Red II is still around, still running on systems that appear to be primarily running at home, in small offices, and in Southeast Asia (based on the times the scans peak). Based on a recent virus report, Nimda is still infecting systems (4.7% of infections), with SirCam at 10.4% of virus occurrences. Both of these involve bugs in Internet Explorer that should have been patched years ago.

The issue with these persistent pests is not so much their nuisance value, but how to go about patching systems that belong to people who either will not or cannot patch them. In many cases, these systems have pirated copies of MS software installed, and their owners may be afraid to visit Microsoft and download the patches. Or the owners remain blissfully unaware that a lot of their network bandwidth goes to scanning and spamming other sites around their world.

It's not just Windows users, either. Installations of Linux from old CDs remain one of the biggest targets of automatic scanning today (my firewall logs show that DNS probes are second only to probes looking for open Windows file shares).

The problem of patching systems goes beyond the systems under our control. Sven Dietrich goes so far as advocating attacking "the immediate surroundings of the attacker," or using a version of an attack, like Code Red, to install the correct patch (Code Green). While such attacks violate the laws of most countries, we might someday reach the point where they will seem justified. After receiving 176 spam emails in a single night (92% spam that night) and seeing my firewall logs filled with denied probes, I am beginning to believe that Sven has a good point.