ROB KOLSTAD

motd

PERHAPS ALL IS NOT ROSES

Dr. Rob Kolstad has long served as editor of *;login:*. He is SAGE's Executive Director, and also head coach of the USENIX-sponsored USA Computing Olympiad.

- *kolstad@usenix.org*

AS I EXAMINE THE EMPLOY- ment scene with the new SAGE salary survey, I can't help but be struck by the hottest field around: security.

I have given security tutorials and the occasional apocalyptic keynote, including warnings about Internet kidnappings. No question, the citizenry of the Net includes an unsavory element. However, I am continually frustrated at the amount of unseemly behavior that permeates our everyday computing experiences—potentially running through the entire IT industry.

Let's try to take an unbiased look at the current state of affairs.

First, let's open our emailbox. Look at that. There are about 45 legitimate messages mixed in among 403 unsolicited electronic mails. While the spam is educational in its way—what with its stock alerts, pharmaceutical announcements, beauty and body enhancement tips, reminders that I could perform a bit better in personal relationships, lottery winnings, and the occasional plea to support our brethren in Nigeria—I must confess that most of it lost interest for me after the thousandth repetition.

How did this incredibly sorry situation emerge? My guess is that no one person or entity feels sufficiently harmed by it to make it stop. Important emails buried (or hidden in a spam folder), decreased ability to find important email, and, one must believe, a certain amount of fraud: none of these is enough to warrant more than an Act of Congress that has been, in my humble opinion, not quite as effective as perhaps its framers had hoped. The cost of spam is hard to determine, since the fundamental rule of accounting ("Costs are as costs are accounted") can lead to wildly divergent answers. In my life, though, where I keep track of the number of daily invasions of my privacy and try to ensure that I don't lose any important email, spam is a truly depressing and time-consuming part of every day.

I don't think this is reasonable.

Let's fire up the Web browser now.

A pop-up! It must be really important. Why else would my time and attention be so violently taken away?

It's another home loan advertisement. I don't need another home loan. I don't need another Web camera. It's astounding the number of things I don't need. Pop-ups might be a necessary evil like advertisements on commercial television and radio, but I hate them. Turning them off in my Web browser made me feel as if my life had improved.

"My computer is so slow these days," says my friend John. A quick check reveals 600 viruses. Apparently, he tends to let Web sites entice him to download software that infects his computer. Removing all those extra features brought his performance back in line.

By the way, the use of "infection," "viruses," and the rest of the biological/health care vocabulary that surrounds this part of a security discussion strikes me as unfortunate. I think many people believe that, like human germs, computer viruses just emerge somehow in the wilderness and make their way to computers. We can't cure the common cold, and computers get sick, too. Makes sense, doesn't it?

Nothing could be further from the truth, of course. Humans engineer these viruses. The more helpful humans not only teach others how to write them but

also create Web sites that enable less skilled individuals to craft their own invaders by point-and-click. On a bad day, viruses propagate through email dramatically more quickly than through the Web.

I don't think this is reasonable.

I asked my security officer how we were doing. "Everything is great," he replied. "The firewall is stopping all the port-scans and we're all patched as of yesterday's new software."

"Port scans?"

"Sure. A few thousand times every hour, various systems try to see if any of our network services will let them break in. Sometimes we get more than one scan per second."

Now why in the world am I being scanned the as many as 100,000 times per day? Why do articles report that un-patched PCs can survive uninfected for no more than ten minutes after being connected to the Internet?

I just don't think this is reasonable. Imagine finally completing the driveway to your shiny new house. Within seconds, a host of people surround your manse rattling every doorknob, trying to open the windows, peering into your basement. Would you put up with this? Even if the people said, "We only want to look"? Of course not.

I asked the security officer about any other anomalies. "We did have a few zombied PCs, but we've reloaded them."

Zombied PCs are PCs whose resources are hijacked by someone, usually for nefarious purposes such as port scanning and spam transmission.

I don't think this is reasonable.

How did all this come about?

I suppose it came a little at a time. Cantor and Siegel opened the floodgates for "commercial use of netnews." Many well-intentioned folks didn't want to trample on free speech, so, after a few years of evolution my emailbox is inundated with offers I don't care to receive.

When challenged about innovative protocols that enabled strangers to email executable code to unsuspecting users, the world's most profitable software vendor said, "Customers are demanding these features" to enhance their experience. Those in power ignored the security folks who said, "This is a bad idea." As predicted, here we are.

Maybe the world's most profitable software company could raise its priority level for security? Oh. Never mind.

Perhaps we should heed those pundits who tell us that FireFox, Linux, *BSD, etc., really just aren't as secure as more popular software. Maybe not. My experiences simply don't bear this out.

The hell of it all is: Everyone can pay (for a spam filter, a virus scanner, a firewall, or higher costs for network bandwidth) to mitigate the security problem. Don't kid yourself if you're an end user, though; someone is paying the money on your behalf and, ultimately, it comes out of your pocket.

What are we to do?

I am afraid that these problems will jeopardize our industry's progress. To start with, not only do we need to educate ourselves and the public about the high costs of security, but we need to understand an important point: Adding security—with its expense in time and money—only gets us back to where we should have been in the first place. An ever-growing security budget yields no growth in usability (usually just the opposite) and no increase in performance or return on investment (unless you count avoiding the potential additional costs of incursion or data theft). This seems wrong.

In addition to education, I believe we need to increase social pressure to influence and to punish evil-doers who penetrate systems, steal my time, and require an entire new US$20B industry just to enable computer users to employ their systems as they were intended to be used.

Legal actions? Civil actions will not result in the deterrent effect that a round-up of a dozen spammers and system crackers might have. Put each of them in jail for a decade or two, and I imagine would-be hackers might think twice. This trend has begun with the conviction and nine-year sentence of a U.S. spammer.

Do ISPs bear any responsibility? I think so. I think they can detect some of the systems that are port-scanning and shut down their communications. Australian ISP Telstra Bigpond recently took an action like this because their resources had been strained by zombied PCs.

I am constantly amazed at the mindset of "Solve the problem close to its manifestation" rather than "Solve the problem at its source." Why aren't we going after crackers and spammers with all the force we can muster? Doesn't it matter to anyone? Is the increased cost of using computers just another small, irritating cost? Does no one realize that security problems are caused by actual people being malicious?

I don't think we're being reasonable.