;login:

THE MAGAZINE OF USENIX & SAGE

April 2001 • volume 26 • number 2

inside:

SYSADMIN
Musings

USENIX & SAGE

The Advanced Computing Systems Association &
The System Administrators Guild

musings

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>

Tech stocks crashed, and I didn't leap from my office window. Not that it would have done any harm, since my office is on the ground floor. But it was amazing to watch as the paper value of my retirement fund plummeted. Alan Greenspan successfully punctured the tech stock bubble, while the President was talking the US into a recession so he can justify a tax cut (which will take effect long after any recession has ended). What a way to begin the millennium!

I was fortunate enough to be able to attend the LISA conference in New Orleans, which despite some rainy weather was still a respite from an unusually cold winter. Global warming, yeah sure! Please do not take me wrong, as I am thoroughly convinced that pumping carbon dioxide, particulates, and other compounds into the air for a hundred years has a measurable effect on climate. If you can see plumes of pollution from space (you can), it is easy to believe that the human race has had a measurable effect on climate. Today, we dump stuff into the atmosphere and hope that it will dissipate – just like people used to do with their sewage by dumping it into large bodies of water. Someday, our techniques for getting rid of gaseous waste will look just as absurd and primitive.

But I digress. The fourteenth LISA conference provided an embarrassment of riches – three tracks instead of two. In other words, there were two invited talks tracks competing with the paper presentation track, and it was devilishly hard to choose which session to attend. Given my personal focus on security, you probably can guess which sessions attracted me the most. Also, I know I can read the Proceedings, and unless I have a Peter Honeyman-like question to ask the poor paper presenter, I often decide to listen to an IT that will not appear in conference handouts.

If you missed LISA, get the Proceedings. I liked the FOKSTRAUT paper about extending Samba to handle "Windows machines determined to tell us their local passwords before attempting to give us the one we wanted." Although the solution, which involves caching those local passwords, sounds really scary, Beck and Holstead (University of Alberta) do recognize the problem and use a dedicated server, carefully secured, for this task.

The very next paper, "Designing a Data Center Instrumentation System," forced me to face a facet of security that I have blissfully ignored. For years I have been suggesting that people take advantage of all the floor space freed up in raised-floor areas that used to hold mainframes. By putting servers in secure areas, they can fix one of the biggest weaknesses in local security, physical access. After all, any UNIX or NT system administrator knows how to get access to any file on any server without knowing any passwords, right? Just reboot with the appropriate installation CD (or a floppy boot disk) inserted in the target system. Moving the systems to a secure area fixes the problem.

Er, except that it turns out that having people near the servers has been important as well. For example, I know what my servers sound like, so if a fan or hard drive bearing begins failing, the noise it makes is quite different than usual and I can do something about it before it becomes a catastrophic incident. Now, move those servers into a data center with servers behind glass rackmount doors, and "even the piercing sound of a piezo-electric alarm two rows away is drowned out" (to quote the paper).

The solution, developed by Bob Drzyzgula of the Federal Reserve Board, involves both "easy stuff and hard stuff." The easy stuff includes things you might already have thought of, like connecting all the serial console ports to a terminal server, and using

SSH for secure remote administration via the terminal server (which might be a Linux or BSD x86 system with multiport serial cards installed). The hard stuff was monitoring other problems, such as temperature, DC voltages, AC current, fan rotation, LED states, and control functions (such as a relay for reset or power on/off of the monitored devices). Drzyzgula chose to design his own boards based on an off-the-shelf microcontroller, and to use RS-485 (the basis for differential SCSI busses) for the physical communication layer. If you enjoy hardware-based approaches, and are not afraid of soldering irons, you should read this one.

The All-Electronic Home

The monitoring paper leads nicely into a really fun IT, given by Lorette Cheswick, assisted by her charming husband and one other family member. For those of us who have not visited the Cheswick home in lovely, suburban New Jersey, Lorette filled us in on just what you can do given an unused intercom system and a willingness to visit the local Radio Shack store and write some scripts. Ms. Cheswick described the amazing talking doorbell and using the intercom to deliver text-to-speech messages to her children, like "the school bus is leaving in five minutes."

I particularly liked the interface that takes Caller ID and turns it into the caller announced, another text-to-speech application. Bill Cheswick has written scripts that announce the closing values for the Dow as well as alerting the family to interesting astronomical events that can be seen from their yard (as well as when to go outside and where in the sky to look). When I suggested the "talking computer voice" to my wife, I got a big no. But then, she was the person who asked me (forcefully) to move the oscilloscope and the frequency generator out of the dining room, which was probably a good idea.

Still, having a voice announce telephone callers (instead of squinting at the Caller ID LCD) is appealing to me. So is being able to see who is at the front door and being notified that the garage door is (still) open, both things that the Cheswicks' system does. Having the NASDAQ closing value announced has been too depressing lately to think about, but I did start thinking about other things I would like to do. For example, I want to install CAT 5 cable when I have my house remodeled. Even if Drzyzgula does make good points about RS-485, CAT 5 does have certain advantages.

For instance, you can transmit power over CAT 5. I knew there were "unused" lines in the four pairs of twisted cables in CAT 5 and learned that people are now using these for sending power to devices that are not big consumers. My local Cisco rep sent me an announcement about "inline power over Category 5," as it is required for the Aeronet 350 wireless LAN. Personally, I am not interested in broadcasting over microwave bandwidths throughout my house, and will be happy to stick to wires. The Cheswicks largely use X10 controllers, which use the house's existing 110 volt circuits as a bus, and their intercom system, which my house just doesn't have.

The New Borg Look

Dkap, a USENIX member who still appears to be our only Borg, showed up in New Orleans with a new look. Instead of the Private Eye display, which dominates one eye and includes a rotating mirror for scanning, he had a Kopin display, a one-quarter VGA full-color display that takes up about a one centimeter square area in front of one eyeglass lens. The Kopin display is a great advance over the Private Eye; it's easy to view (he unclipped the display and shared it with many attendees), but the one-quarter VGA means xterm windows that can hold only 40 characters per line. And the Kopin costs as

When I mention wearables, many people respond "Yuck, who would consider wearing their computer?," and then their cell phone starts ringing.

much as a 17-inch LCD monitor (at a quarter the resolution). But prices should come down.

The rest of the rig now fits into a vest and includes two separate processors, the main server (which supports the Kopin display through an FPGA) and a disk server based on an IBM Microdrive. The two processor boardlets communicate using 100BaseT, and the power bus uses the power over CAT 5 I just mentioned. There is also an I^2C bus for peripherals, including wireless (802.11), cell phone, IR, and GPS. The entire rig, as worn by Dkap, weighs under two pounds, and he claims as much as 20 hours without recharging (try that with your laptop). The Web page for the new style wearable is *<http://www.media.mit.edu/wearables/mithril/>*.

When I mention wearables, many people respond "Yuck, who would consider wearing their computer?," and then their cell phone starts ringing. During the call, they pull out their Palm and consult their schedule, make a note, then put away the two computers they have just used. Yeah, who would want to wear a computer in public?

Dkap and the Mithril design still use the Twiddler, which I consider a terrible design for a one-handed keyboard. Chording keyboards should be designed for human fingers. Curl your fingers halfway, and place them on a desktop, and you'll notice they form an arc, not a straight line. The Twiddler is designed so that both right or left-handed people can use the same device, so it has straight lines of buttons like the left hand of an accordion. I hated that when I played the accordion and can't imagine picking it up again. There are other chording keyboard designs out there.

Security

Part of the LISA third track was devoted to security. I really enjoyed both Steve Romig's and Tom Perrine's practical advice about handling security incidents that involve the police. I had heard Ches' "Mapping Corporate Intranets" talk at a security conference, but recommend it as interesting if you have not already heard it.

And beyond LISA, things are still popping. January brought with it four new BIND security bugs, three providing buffer overflows. Someday, Rob Kolstad (if he is still running the LISA Game Show in the distant future) will be able to use a box under the Security column labeled BIND. The question will be, "What critical component of the Internet was also the most widely exploited server software in the year 2000?" Actually, this should read ". . . between 1998 and 2001?"

The announcement of more buffer overflows in BIND set up a storm of criticism about the Internet Security Consortium, the maintainers of BIND (isc.org>). In the end, Paul Vixie amply defended ISC, pointing out that any large body of code is bound to have flaws, and the BIND version 9 has been completely rewritten. Still, the important point I want to make is if you have ANY servers running older versions of BIND, replace them. You can convince BIND servers to cough up the version number in most cases by using:

```
dig @serverip version.bind. CHAOS TXT
```

where @serverip is the address of the DNS server you want to query. Note that script kiddies everywhere already know how to do this, or have scripts that do it for them, so you won't be the first to do this if you have any public DNS servers.

Summary

This issue of *;login:* contains summaries of LISA, so you should read them (and the Proceedings) if you want to learn more.

To summarize my own column, I'd like to remind you all that most people alive in the world today have, by definition, average intelligence. This is a no-brainer, right? Sure, until you try using some off-the-shelf software designed for those average users. About 18 months ago I wrote that the best user interface ever designed is the light switch: a simple-state machine with an obvious interface and a quick and appropriate response to the user's interaction.

While things will have changed by the time you read this, Northern California is still having rolling blackouts to deal with the decision to deregulate electricity in California and how the free market took advantage of this wonderful opportunity. The result, which has practically bankrupted billion dollar utilities like Pacific Gas and Electric, has led some people to suggest reviving nuclear power as a "clean option" to fossil fuels. Let's think about how we have dealt with the waste products of this clean option.

One by-product of nuclear reactors is plutonium, with a half-life of more than 20,000 years. Designing something that can safely contain plutonium for this time span has proven beyond our current capabilities. The best solution so far is to put the plutonium into nuclear warheads, which then must be carefully stored in highly secured areas because they are so dangerous.

Another option for dealing with so-called "depleted uranium" is to shoot it at your enemies as anti-tank ammunition. The US has managed to transfer over 30 tons of radioactive material to the Middle East this way. The people who came up with this solution to the nuclear waste problem should be given some kind of award.

Again, I digress. I consider it my responsibility, and hopefully yours as well, to act as intelligently as possible in an uncertain world. And don't forget to update BIND.