

RIK FARROW

musings



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* and editor of the SAGE Short Topics in System Administration series.

■ rik@usenix.org

NOTE

[1] There actually were two papers presented about security at HotOS, so security was a topic that was seriously addressed.

AT MY HOUSE, AS AT MOST OF THE buildings in the world, the best views are from the roof. When I sit up there, I can see thunderstorms 30 miles away, up on the Colorado Plateau to the north. Even though I can see great bolts of lightning striking the ground, around me it is quiet and calm.

The comparative silence is an illusion. As I wrote in my last column, enormous botnets wait to carry out their owners' bidding, whether it be DDoS, relaying spam, or assimilating more systems. There is more bloated software than ever before, just waiting to be exploited. Steve Manzuik has an article in this issue about security software that has been (and still is being) exploited.

One of the things I have always found fascinating is operating system design. I will have attended the HotOS workshop, as an observer, by the time you read this. And one aspect of operating systems that I don't expect will be discussed is security [1]. We have generally chosen not to include security in our operating systems, outside of jails, firewalls, and some coarse-grained protection like the BSD secure levels. And these are add-ons. Operating systems are not designed for security; they are designed for performance and to support features.

Computers are already ubiquitous. From the simple controllers in toasters, microwaves, and cars to the more powerful ones in cell phones, computers have become embedded throughout the developed world. What is changing about these computers is just how powerful they can be.

AMD has announced a new, low-power, i386-compatible CPU, the Geode LX 800 (<http://www.linuxdevices.com/news/NS2872282951.html>). This link points to a Linux site, but if you read the AMD PR, it points out that the Geode supports a familiar programming environment—Windows CE. The Geode can amply support Windows or Linux or BSD. The 500Mhz processing core includes native support for DDR RAM at 400Mhz, L1 and L2 caches, 2-D graphics, and hardware support for cryptography. The companion chip supports ATA, PCI, and USB busses, and the two chips together draw only two watts of power. Compare that power consumption to almost anything on the desktop today, along with the performance, and you can see where this is going. Cell phones with the same capabilities as PCs of five years ago—except without decent keyboards.

And security? I would not want to carry any device, especially one designed for network communications like a cell phone, that runs Windows CE. But even

getting FreeBSD, OpenBSD, or Linux to run mobile applications securely takes some serious work. None of these operating systems was designed from the ground up to support security. Security was included, in the case of UNIX, to support multiple users on the same system, not for protecting a single user who might run hostile apps.

Perhaps you don't believe me. Let's look at some solutions.

Sandbox

The BSD jail is a nice solution: Chroot on steroids, something I've written a lot about before. Its failings are limited control over networking and none over processor scheduling.

Fedora includes a complete SELinux configuration. SELinux was designed to provide Mandatory Access Control, a mechanism where users are not able to control even access to their own files. The configuration is byzantine but will work out-of-the-box, as long as you only want to run applications that are also out-of-the-box. If you want to run third-party applications—for example, a cell phone app for a distributed game, online trading, or authentication for credit card purchases—you or the application developer must write your own policy. And if the application developer has written a buggy app, should you expect that they have written a robust policy?

The Linux kernel hooks for SELinux do support other policies. That is, someone could replace the policy mechanisms that come with SELinux with their own programs, and have policies more suitable for a secure mobile device or other embedded system. I believe this approach deserves more investigation.

Then there are Virtual Execution Environments (VEEs) like Xen. You can read about Xen in this issue, and see that the designers do intend it as a method of providing a secure environment for sharing your computer with others. Essentially, Xen provides complete virtualized systems where you can run a guest OS that can be part of a computing grid.

Or you could run your Web browser/mailtool in its own environment, leaving little for these complex programs to compromise if and when something goes wrong. I'd like to do that.

Of these solutions, only Xen comes close to providing a secure environment from the ground up. And even with Xen, you are still stuck with managing a firewall at the monitor layer that prevents a compromised virtual machine from misbehaving on the network. But I do believe that Xen is a great step forward.

Another Hat

In my collection of work apparel, I have added a new hat to wear, that of editor of *login*. I can't rely on distant visions from my rooftop to learn what the USENIX community wants or needs, or what people within that community are doing. I need you to tell me what interests you, what you want to know, what you are doing, or, better yet, what you can share with the community. The SAGE update, written by David Parter, is one example of learning what part of the community is doing.

Although united around computing, the USENIX community is a broad one. A quick look at the events calendar shows that there are many small conferences/workshops sponsored by USENIX, often co-sponsored with other organizations. These workshops cost more than can be collected as registration fees, and the USENIX Association—that is, you—supports these workshops and small conferences. This is part of the reason why you will find the summaries in the back of most every issue of *login*, so that you can discover what is being done with your support.

But there is more there than meets the eye. The obvious purpose of many conferences is so that academics can get papers published in proceedings. The deeper goal is that this research will lead us in new directions, to truly advance both the science and the practice of computing. This research ranges from better ways to configure systems, distribute loads, support mobile systems, and, yes, even create secure systems that can safely execute untrusted code without requiring geniuses from within the NSA to configure the policy.

In this issue I have included several articles relating to security to complement the Security Symposium, which takes place the first week of August. Abe Singer's opinion piece is particularly relevant, as there will be a panel about this very topic on Thursday, August 4.

Security is an easy topic for me, my home territory. It is when I venture into unfamiliar territory that I really need your assistance.

As I wrote a moment ago, the USENIX community represents a wide array of interests. Many members are system administrators, an area I am familiar with. But there are many other areas where I am on shaky ground: operating system design, mobile networking, measurement, sensor networks, middleware, distributed systems, and Virtual Execution Environments. If you look at the USENIX events calendar (<http://www.usenix.org/events/>), you will see that all of these topics are represented by conferences or workshops

(some already over by the time you read this). I want to expand the coverage in ;login: to more of these topics, while not abandoning what has been popular in the past.

You can help me by volunteering to read drafts of articles. I appreciate the advice of subject matter experts (SMEs), and really need the advice to be the best possible. Even more, I welcome SMEs who are willing to write about what excites them, so they can share this excitement with the larger community. It is this, the joy of expanding into interesting but unknown territory, that got me interested in USENIX conferences in the first place.

I am also looking for book reviewers. If you would like to review books for ;login:, send me a short email telling me exactly what topics you are interested in. You don't have to be an expert, just have a strong interest and enough experience to tell whether an author is providing you with accurate and useful information.

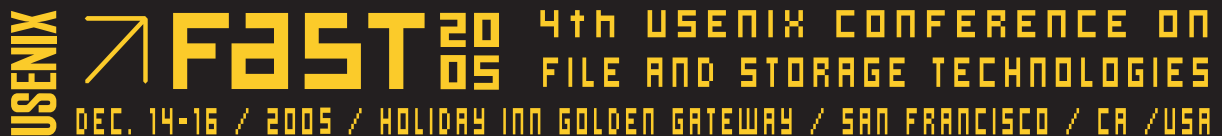
This issue includes an article by Adam Levin about his experiences learning about supporting an Oracle application with NAS or SAN. I would like to publish other articles in this vein, where you can share your experi-

ence with a practical undertaking that involves installing and configuring software, hardware, and/or networking to solve a particular problem. I will be looking for proposals (see Writing for ;login:, <http://www.usenix.org/publications/login/writing.html>) that will be of benefit to as much of the community as possible. I chose Adam's article based on questions that came up in the SAGE mailing list and my own curiosity about the practical implications of implementing SAN or NAS solutions.

So please let me know what you are thinking. You can email me: send me article proposals and offers to write book reviews. You can also look for me at USENIX conferences, because I attend as many as I can. I am easy to identify: there aren't that many tall bald guys with ponytails wandering about.

The USENIX Association is really about a community, a very large and varied community spread over the world and covering many specialties. I want to support this community as best I can.

I will do a better job of it with your assistance and support.

The logo for the 4th USENIX Conference on File and Storage Technologies (FAST '05). It features the USENIX logo on the left, followed by a stylized arrow pointing up and to the right. The word "FAST" is in large, bold, yellow letters, with "2005" in smaller letters to its right. Below "FAST" is the text "4th USENIX CONFERENCE ON FILE AND STORAGE TECHNOLOGIES" in yellow. At the bottom, it says "DEC. 14-16 / 2005 / HOLIDAY INN GOLDEN GATEWAY / SAN FRANCISCO / CA / USA" in yellow.

USENIX **FAST** 2005 4th USENIX CONFERENCE ON
FILE AND STORAGE TECHNOLOGIES
DEC. 14-16 / 2005 / HOLIDAY INN GOLDEN GATEWAY / SAN FRANCISCO / CA / USA

SAVE THE DATE!

4th USENIX Conference on File and Storage Technologies

December 14–16, San Francisco, CA

Join us in San Francisco, CA, December 14–16, 2005, for the latest in file and storage technologies. The 4th USENIX Conference on File and Storage Technologies (FAST '05) brings together storage system researchers and practitioners to explore new directions in the design, implementation, evaluation, and deployment of storage systems. Meet with premier storage systems researchers and practitioners for 2.5 days of ground-breaking file and storage information!