;login:

THE MAGAZINE OF USENIX & SAGE

June 2002 volume 27 • number 3

inside:

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*

Like every other USENIX member, I am always learning. The resources appear endless: new books, classes, online Web pages, mailing lists, magazine articles, and questions that people send me.

Just the other day somebody emailed me hoping I could tell her how to change the admin password on the used notebook running XP she had just acquired. I checked out my old favorite, a Linux boot floppy that enables you to change any password on a Windows NT system, and discovered that it won't work for Win2K. At least the site with the bootdisk is still around (*http://home.eunet.no/~pnordahl/ntpasswd/bootdisk.html*).

The buzz for a while now has been attacks on Cisco routers. Now, you probably all remember that Cisco has had its share of security woes (not an unreasonable burden, but still there). What has changed has more to do with rumors than reality – at least so far.

One rumor is that the source code for IOS, Cisco's Internetworking Operating System, has been stolen. That rumor dovetails nicely with a second rumor, that a rootkit for Cisco routers is in the wild. Rootkits for UNIX systems have been around since at least 1994. The "original" rootkit ran on SunOS, included trojaned commands that hid the existence of a sniffer and its logfile, and made it easy for the installer to return and upload the logfile. Some people really appreciated rootkits, as they were busy installing them on every open system they could find – particularly at ISPs.

ISPs made dandy places to install rootkits, especially in the mid-'90s. Small ISPs would install a UNIX mail/Web server, and the attacker would load the rootkit on it. The UNIX server also would sit on a broadcast network, so any transit traffic would be sniffed as well. Of course, the accepted practice today is to put servers on their own subnets and to use switches instead of hubs. Not that hubs are a proven way to prevent sniffing. Check out angst (*http://angst.sourceforge.net/*) if you don't believe me.

The notion of a Cisco rootkit disturbed me at first. I guess I just didn't like to think of a router as something running a vulnerable OS with vulnerable services. But, of course, routers run operating systems. Cisco has written their own. Juniper Networks uses a modified version of BSD.

O'Reilly keeps publishing books, and occasionally sends me a copy, which I much appreciate. *Hardening Cisco Routers*, by Thomas Akin, seems very appropriate for these days. And, Akin's tome secretly pleased me as well, because it covers much of the same turf that I once did in a router security class – but in more detail. For example, I didn't realize that the difference between logging into a Cisco router and what you can do after entering the enable password is based on privilege levels. You can actually set up user accounts (if you are using TACACS or RADIUS) with different privilege levels, then configure the router to provide access to sets of commands at any of the 16 different privilege levels. I had heard that IOS runs at a single hardware privilege level, and the notion of software configurable access to commands agrees with this. IOS is its own "secure" OS, although without the usual aid of hardware support. Like running a shell within the kernel.

Akin takes you through the hardening process succinctly, starting with a description of the issues, going into access control, passwords, remote authentication servers, logging, disabling dangerous protocols/services, controlling routing protocols, and even physical security. I had hoped there would be more on BGP4 filtering, but the focus was more on not accepting or distributing routes via Interior Gateway Protocols (IGPs), and setting up connection authentication with BGP4. I have always wanted to have all of the security documentation for Cisco routers in one place. While *Hardening* does not include the firewall features of Cisco routers (other than rate limiting for DDoS attacks and which ICMP packets you can consider dropping), it admirably covers its topic area. And at 172 pages, it's a quick read, too.

The other oft-rumored "big attack" on routers involves BGP4. BGP, Border Gateway Protocol, is the glue that holds the Internet together. Unlike IGPs, BGP uses Autonomous System (AS) numbers to describe routes. An autonomous system is a collection of networks under the technical control of a single agency. The way I think about how BGP works is this. Each AS has routes to many networks that belong within that AS, their netblocks (see arin.net, ripe.net, apnic.net for the various AS and netblock registries). An AS advertises routes to their many networks via their AS number, rather than as specific routes through a list of routers. That makes routing within an AS transparent to sites outside of the AS. You just get the packets to the border of the AS, and the AS handles routing the packets to their destinations.

Of course, this setup implies that each AS must be using an IGP internally, so that its own routers know the actual routes to each supported network. What BGP4 does is takes the information from the IGP routing advertisements, converts it to BGP4 advertisements, and shares this with the BGP-speaking neighbors. Only updates are distributed, as every update must be exchanged with every BGP4 speaker. Unstable networks result in frequent changes, or route flapping, wasting not so much network bandwidth as router CPU cycles.

Okay, so BGP4 is the glue and seems to be working just fine. What's the problem? A nice answer to that is AS7001, in April 1997. AS7001 was the AS number for a small ISP in Florida, a Sprint customer. This ISP made a mistake in configuring BGP advertisements so that all the routes that were being advertised internally were forwarded to Sprint using BGP4. As I understand it, this little ISP began advertising itself as the best route for many Class C networks, and as soon as this route spread, the link between Sprint and this little ISP became flooded. Imagine, if you will, the US airline system of spokes and hubs, and now Santa Rosa, California, has announced it has taken the place of San Francisco International, Atlanta Hart, Washington Dulles, Chicago O'Hare, etc., and all the traffic heads there. It was not a pretty picture.

Cooler heads prevailed. By examining the BGP routing updates, someone noticed that AS7001 was declaring itself the best route for networks having nothing to do with it, and filtered all updates coming from AS7001. The problem stopped once people started filtering (blocking) updates from AS7001, and gave Sprint a chance to help the little ISP fix their problem.

The AS7001 incident helped make NSPs aware of how crucial BGP filtering is. Configuring BGP4 routing and filtering is an art form, and not practiced by many (compared to the number of network admins there are). We haven't had a similar problem in years. Also, it is standard practice today to either use dedicated links between BGP4 neighbors, or include an MD5 digital signature with each packet, to prevent spoofing, resetting, or hijacking of the connection between BGP4 neighbors, which stays up as long as the link and routers are up.

This brings me back to where I started: potential, wide-scale attacks on routers. If many routers can be penetrated and rootkits installed, then these routers become simi-

Configuring BGP4 routing and filtering is an art form, and not practiced by many.

As a rumor-monger, I am strongly suggesting that you see to the security of any routers under your control.

lar to the agents used in DDoS attacks. If these routers begin sending incorrect BGP4 updates on command (from authenticated routers, mind you), then considerable disruption of the Internet will occur. With no one suspecting that their router has been corrupted, and general Internet connectivity being disturbed, well, things could get messy for a day or so. Just remember the original Internet Worm. If you want to read more on this, check out "Origins of Internet Routing Instability," by Craig Labovitz et al. (Arbor Networks): *http://www.comsoc.org/confs/ieee-infocom/1999/papers/*. BBN and others have suggested using digital signatures on every update, but if the routers are subverted, the digital signatures will authenticate the phony advertisements as well. You can learn more about the BBN solution, secure BGP, by visiting their Web page: *http://www.ir.bbn.com/projects/s-bgp*.

Note that this is not just a problem for router vendors. You can run BGP4 on Linux and BSD systems as well (MRTD, *http://www.mrtd.net*, and Zebra, *http://www.zebra.org*). And we know that these systems are always totally secure.

Of course, all this is fantasy and rumors right now. As a rumor-monger, I am strongly suggesting that you see to the security of any routers under your control. The little whispers I have been hearing remind me a lot of what was being said before the DDoS attacks of February 2000 occurred, and I really thought I should mention this.

## USENIX Needs You

People often ask how they can contribute to the USENIX organization. Here is a list of needs for which USENIX hopes to find volunteers (some contributions reap not only the rewards of fame and the good feeling of having helped the community, but authors also receive a small honorarium). Each issue we hope to have a list of openings and opportunities.

- The *;login:* staff seeks good writers (and readers!) who would like to write reviews of books on topics of interest to our membership. Write to peter@matrix.net.
- The *;login:* editors seek interesting individuals for interviews. Please submit your ideas to *login@usenix.org*.
- *;login:* is seeking attendees of non-USENIX conferences who can write lucid conference summaries. Contact Tina Darmohray, <*tmd@usenix.org*> for eligibility and remuneration info. Conferences of interest include (but are not limited to): Interop, Internet World, Comdex, CES, SOSP, Ottawa Linux Symposium, O'Reilly Open Source Conference, Blackhat (multiple venues), SANS, and IEEE networking conferences. Contact *login@usenix.org*.
- *;login:* always needs conference summarizers for USENIX conferences too! Contact Alain Hénon *ah@usenix.org* if you'd like to help.
- The *;login:* staff seeks columnists for:
  - Large site issues (Giga-LISA),
  - Hardware technology (e.g., the future of rotating storage)
  - General technology (e.g., the new triple-wide plasma screens, quantum computing, printing, portable computing)
  - Paradigms that work for you (PDAs, RCS vs. CVS, using laptops during commutes, how you store voluminous mail, file organization, policies of all sorts)

Contact *login@usenix.org*.