July 24, 1997

Watching Big Brother

Just get right tools for monitoring networks, view electronic world at work / **Simson L. Garfinkel**

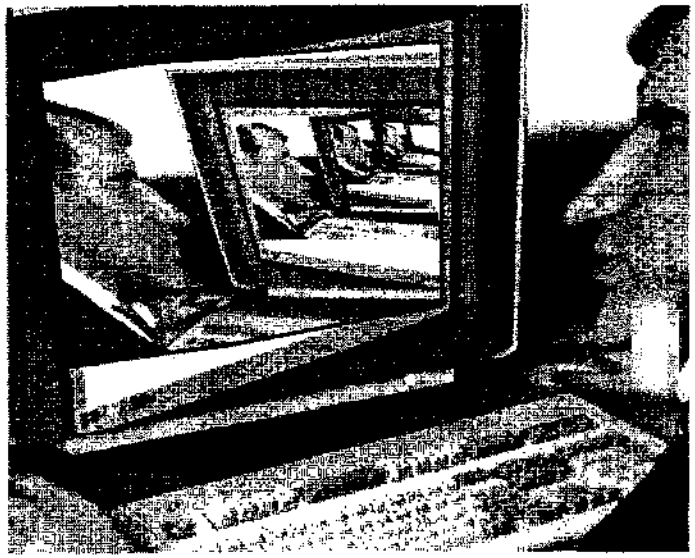
IF YOU ARE TIRED OF having big corporations watching your every move on the Internet, downloading cookies into your Web browser, building profiles of your habits, and generally invading your privacy, why not turn the tables on them?

I'm not suggesting that you hack into corporate databanks and download confidential files – that's unnecessary, not to mention illegal. Just sitting with an ordinary dial-up connection to the Internet, there's a lot you can learn about the state of the electronic world.

Start with a program called ping, which is built into Windows and most versions of UNIX. The ping command sends a few packets, or signals, to another computer on the Internet, listens for a response, and then prints the round-trip time.

If you keep a log of how long it takes to ping well-known locations, such as www.netscape.com and www.whitehouse.gov, you can see how congested the Internet is between you and that site at any given time. By comparing your notes with friends, you can find out who has a better Internet service provider.

If you want to learn where the delays are actually coming from, you'll want a program called traceroute. This program sends a series of packets to a remote host and uses them to map out the path



taken and the delays encountered.

Traceroute programs are valuable debugging tools for network administrators, but they're also useful for noisy consumers. The program is built into UNIX. If you are running Windows or Mac OS, there are a variety of shareware programs you can download. On Windows, I like NetLab, which has various features including "finger," "whois," and "ping." Some Web sites also have traceroute servers; a particularly nice one is operated by PCSLink, an ISP in Arizona. It's at http://www.pcslink.com/cgi-bin/trace.

WhatsUp and WhatsUp Gold are two powerful network monitoring programs from Ipswitch, a small software company in Lexington. The program is designed for corporate networks. WhatsUp will seek out your servers and workstations, draw a map, and then continually check the machines to make sure everything is working. The program will also monitor particular network services, such as your Web server or name server. And it will draw graphs and piecharts showing your network's history.

The Gold version allows you to monitor many networks at the same time, and is set up so that other people in your organization can also view a network's current status. You can download a free demo from http://www.ipswitch.com/.

When you install WhatsUp, the program prints an interesting message: "Please do not monitor network elements that you do not have control of without the expressed permission of the owners of those network elements."

The reason for this warning, says Roman Kichorowsky of Ipswitch, is that if lots of people start monitoring a Web site at the same time, it can cause significant problems. For example, if 10,000 people decided to monitor The Boston Globe's Web server every minute, just to see whether it was still running, that would generate an extra 1.4 million hits every day.

Indeed, unauthorized monitoring once put Ipswitch's chief technology officer, John Junod, in the hot seat. Apparently, somebody in Europe was using Junod's ping program to monitor the National Security Agency's main gateway to the Internet. Unfortunately for Junod, the program was helpfully putting his name and copyright message into each packet. It wasn't long before he got a call from an angry network administrator at Fort Meade, Md. The United States' foremost spy organization was not amused.

Notwithstanding this warning, I've been using WhatsUp to monitor my ISP, my ISP's provider, and parts of the Sprint, MCI, and AT&T Internet backbones. To be fair, I've changed WhatsUp's preferences so that instead of checking each host every minute, I'm only checking every five minutes. The monitoring reveals that there are widespread congestion problems on a day-to-day basis but that most of the problems clear up within 10 or 15 minutes. Unfortunately for network administrators, this sort of intermittent problem is the toughest to track.

Using the Internet's Simple Network Management Protocol, you can do even more sophisticated network monitoring. For example, I can use SNMP to monitor the router in my basement and find out how much of my high-speed connection to the Internet is actually in use and how much is idle. I can connect to my ISP's modem bank and find out how many of the dial-up lines are in use. I've even connected to Web servers in New York and discovered that their Ethernet card was getting a large number of communications errors – possibly because of a loose cable or a chip that was about to go bad. SNMP has a built-in security to prevent this sort of eavesdropping, but most Internet users don't know it's there or how to turn it on.

Fortunately, most SNMP programs are too difficult for the majority of Internet joyriders to master. One exception is Dartmouth University's InterMapper. Just give this Macintosh program the name of a computer, and it will automatically create a map of the network, monitor the network, and check all the systems using SNMP. InterMapper even draws moving dots to show you when network links are heavily congested. You can find out more information about InterMapper at http://www.dartmouth.edu/pages/softdev/.

Simson Garfinkel's new book, "Web Security and Commerce," was just published by O'Reilly & Associates. For more information, check out http://www.ora.com/catalog/websec/.