HOTWIRED Wired News Webmonkey RGB Gallery Animation Archives *Wired* Mag Suck.com

Search: HotWired Archives *for* go

50 Ways to Crash the Net

by Simson L. Garfinkel

18 August 1997

On 17 July 1997, the Internet received a critical warning about its future, but that day and its lessons are already fading from memory. On that day, two blunders conspired to shut down the Internet for millions of users.

Early that morning, a system operator accidentally uploaded a corrupt database to the Internet's root domain servers. Until the problem was corrected, it was impossible to send email or access the Web within the .com and .net domains. The Internet was suddenly numeric, like the phone system. Forget about contacting http://www.hotwired.com - anybody trying to get to Synapse couldn't, unless they knew the numeric address of one of HotWired's servers.

The second snafu was more localized, but more severe for those affected. On that same Thursday morning, a construction crew in Virginia inadvertently sliced through a fiber-optic cable belonging to WorldCom and leased to Sprint. Many of Sprint's Internet customers in the mid-Atlantic states and New England couldn't get on the Net at all.

As someone affected by both outages, I spent most of the morning trying to figure out who to blame - and how to get my system operational again. But there was nothing I could do but wait.

The myth persists that the Net was built to withstand the blast of an atomic bomb. But that was the military-run Arpanet of the 1970s, not the corporate-run Internet of today. "What's basically wrong is we are centralized," explains Dr. Peter Salus, Internet historian and author of *Casting the Net.* "We have violated the constraints that the Department of Defense had in 1967."

Indeed, one of the most significant results of commercializing the Internet has been to create more single points of failure, rather than a more redundant and reliable network. That's because companies are busy finding ways to make themselves indispensable: User self-sufficiency is incompatible with sustained corporate profits.

In December 1995, Internet pioneer Bob Metcalfe predicted a global Internet meltdown. Since then, he has eaten his words. Nevertheless, real problems with the Internet remain. What's more, it's increasingly likely that these lurking problems will be deliberately exploited or tickled by accident, and result in another global Internet collapse.

How might it be done? The following 50 ways to crash the Net are based on conversations I had with Gene Spafford at Purdue University, Alan Wexelblat at the MIT Media Lab, Eugene Kashpureff at AlterNIC, and Fred Cohen at Sandia Laboratory's Computer Security Group. Most of these attacks work by targeting a single point of failure within today's Internet. Others rely on creating storms of activity that overwhelm legitimate network traffic.

Click the right arrows below to begin.

(**Please note:** Neither I nor HotWired suggest that you actually *attempt* any of these means of sabotaging the Internet, nor do we condone any such attempts; we merely offer these as frightening - and funny - examples of how vulnerable the information infrastructure we rely on really is.)

Domain name system attacks

DNS is at once vital to today's Internet and poorly designed. Crash it, and you leave the Internet in shambles.

> **1.** Disrupt the domain name system by uploading a bogus database to the root domain servers. (Network Solutions already demonstrated this one.)
>
> **2.** Flood prominent nameservers with requests from all over the Internet.
>
> **3.** Mount host attacks against the machines on which the name servers are running.
>
> **4.** Find a bug in the DNS server that makes the program crash when provided with bogus input. (This happens about once a week at my ISP for no apparent reason, so there definitely *is* a bug.) Exploit continuously.
>
> **5.** Find a bug in the Microsoft Windows 95 DNS client that causes the computer to format its hard drive when resolving a particular URL. Publish that URL.
>
> **6.** Falsify the DNS entries for a major WWW server, like AltaVista, so that people trying to reach these machines are redirected to the DNS port on the root servers. Ouch!
>
> **7.** Buy 10 backhoes.

Router attacks

The diversity of the early Internet is long gone. These days, 80 to 90 percent of the *computers that run the Net are routers manufactured by Cisco Systems. This makes them especially vulnerable to common flaws.*

8. Find a key bug in Cisco's operating system and exploit it.

9. Get a job at Cisco and plant your own vulnerability in the operating system.

10. Convince 50,000 people to ping key backbone routers, resulting in CPU overload.

11. Capture administrative passwords used to access key Internet backbone routers. Break in and change configurations, then change the passwords.

12. Alter each backbone ISP's master router configuration files so that next time the routers are updated, they crash.

13. Block legitimate administrative access to the machines.

14. Insert forged routes into Internet routing tables to take key machines off the Internet.

15. Announce on the Internet's routing tables that your router is absolutely the best router to get to Mae East.

16. Get physical access to key routers in out-of-the-way locations and unplug them.

17. Don't bother with the routers, just unplug the air conditioners.

Critical host attacks

A small number of computers on the Internet are accessed by a tremendous number of people. Attacking these machines can make the Internet unusable for millions of users.

18. Find the administrators of key machines and personally threaten them so they don't come to work. Alternatively, shoot them.

19. Call the phone company and tell them the leased lines connecting key computers are no longer needed. "We're having a new T3 installed from UUNET." Once leased lines are disconnected - even by accident - it can take weeks to get them re-established.

20. Steal the VeriSign master key and issue fraudulent certificates.

21. Flood VeriSign's certificate revocation server with requests. Result: ActiveX applets won't load.

22. Instead of actually breaking into one of these machines, just make it appear that way. Frenzied sysadmins are sure to make catastrophic mistakes.

IP attacks

Internet enthusiasts love to boast about the power of Internet protocol, but in fact ICMP packets have no authentication, which opens up a number of interesting opportunities for exploitation.

23. Send fake ICMP Redirect messages to major sites, causing those sites to send their packets to the wrong destinations. The packets will eventually get to the correct location, but not without causing needless congestion.

26. Send ICMP Quench messages. These tell the major hosts to send out their packets more slowly.

27. Send forged ICMP Host Unreachable messages to a few key machines, telling them that machines with which they must communicate are unreachable.

28. Send ICMP or UDP Echo-virus packets to well-known hosts. Then sit back and watch them tie themselves in knots.

End-user-based attacks

The major limitation of the attacks listed above is their single point of origin. A more effective approach is to trick unsuspecting Internet users into doing your bidding.

27. Run a contest with a US$10,000 reward that goes to the person who stays connected to your Web site for the longest period of time.

28. As part of the contest, give extra credit to users who run a downloadable Web spider and continuously send you the results.

29. Distribute a hostile computer program on your Web page that reads through a person's email address book and sends a copy of itself to each person listed therein.

30. Distribute a hostile applet that disconnects users' modems and calls the unpublished technical-support number of a major Internet backbone provider.

31. Draw people to your Web page by loading bogus DNS entries for popular machines, like home.netscape.com or www.microsoft.com, into prominent nameservers, so that people trying to go to these machines are sent to your Web server. (That's what AlterNIC did to steal www.internic.net.)

32. Distribute easy-to-use mail spamming programs for free.

End-user attacks

Instead of having end users attack the Internet, attack the end users themselves. The resulting calls for help will swamp tech-support lines.

33. Have a hostile program upload bogus firmware to users' modems. Once the modems crash, there is no way to download a fresh copy of the firmware.

34. Have the hostile applet erase the computer's ROM BIOS. (Most new computers have their ROM BIOS stored in `EEPROM`.)

35. Once the hostile program finishes executing, have it encrypt the user's hard drive and print a ransom note claiming that the attack came from the user's ISP.

36. Alternately, don't bother attacking the user's machine - just send out spam mail that appears to come from the user's ISP and asks them to call tech support right away.

Social-engineering attacks

Not all attacks need to be technical. Here are some attacks aimed at the Internet's social fabric. These may not crash the Net so much as strangle it to death.

38. Get Congress to pass CDA 2.0.

38. Convince a major Internet service provider not to carry its competitors' packets unless they pay for the right.

39. Convince a few key senators that the Internet is a US resource that should be exploited for the national good.

40. Convince the National Science Foundation that the Internet is an NSF resource that should be exploited to fund science research.

41. Establish an Internet governance organization that claims to represent all netizens.

42. Establish a second organization that represents all ISPs.

43. Encourage webmasters to unionize and strike.

44. Spam people with death threats to convince them that the Internet is unsafe.

45. Hack Wall Street's computers and set the price of Cisco stock to $1.50.

Insanely huge attacks

When I called up Fred Cohen at Sandia Laboratory's Computer Security Group, I discovered that he has spent years thinking up ways to attack the Internet's infrastructure. Some of his *favorites include:*

> **46.** Create cascade failures on the power grid. This would take out the Internet, and a lot more. Something like this happened in Cambridge, Massachusetts, when more than 200 businesses and hundreds of thousands of users up and down New England lost their Net connections after an explosion knocked out electrical power in large parts of Boston and the surrounding area.
>
> **47.** Create a cascade failure in the phone system by modifying a few bits of code in a major telephone company's switching systems.
>
> **48.** Do a nuclear test above the atmosphere. According to Cohen, a test conducted by the US military in the '50s "took out communications from New York through Sydney for several minutes" by disrupting the magnetic field of the earth.
>
> **49.** Inject power to the earth's field lines at the north and south poles to disable large areas of electromagnetic communications (there is actually a patent on this technique).

In the overall scheme of things, taking out the Internet would certainly hurt. But we are not as dependent on the Internet now as we soon will be, when an Internet crash could delay a military deployment or create financial havoc. Today, says Cohen, if you want to destroy a country's infrastructure, you're better off going after its power stations than its Internet dial-ups.

But that's changing. The Internet is being used for more critical things - and it's a single network, rather than multiple, independent networks, which would have a better chance of withstanding serious attacks. Ten years from now, things could be much worse.

So what's the 50th way to crash the Internet? It's easy, really:

> **50.** Wait until 1 January 2000.

. . . .

Have any of your own theories about the next big Net disaster?

Related links:

Wired News' Toxic on the potential for catastrophic outages.

Wired News on the Millennium Bug.

Email Synapse.

synapse