

Wednesday, December 21, 2005

The Internet Is Broken -- Part 3

Researchers are working to make the Internet smarter -- but that could make it even slower, warn experts like Google's Vinton Cerf.

By David Talbot

This article -- the cover story in Technology Review's December-January print issue -- was divided into three parts for presentation online. This is part 3; [part 1](#) appeared on December 19 and [part 2](#) on December 20.

In part 1, we argued (with the help of one of the Internet's "elder statesmen," MIT's David D. Clark) that the Internet has become a vast patchwork of firewalls, antis spam programs, and software add-ons, with no overall security plan. Part 2 dealt with how we might design a far-reaching new Web architecture, with, for instance, software that detects and reports emerging problems and authenticates users. In this third part, we examine differing views on how to deal with weaknesses in the Internet, ranging from an effort at the National Science Foundation to launch a \$300 million research program on future Internet architectures to concerns that "smarter" networks will be more complicated and therefore error-prone.

The Devil We Know

It's worth remembering that despite all of its flaws, all of its architectural kluginess and insecurity and the costs associated with patching it, the Internet still gets the job done. Any effort to implement a better version faces enormous practical problems: all Internet service providers would have to agree to change all their routers and software, and someone would have to foot the bill, which will likely come to many billions of dollars. But NSF isn't proposing to abandon the old network or to forcibly impose something new on the world. Rather, it essentially wants to build a better mousetrap, show that it's better, and allow a changeover to take place in response to user demand.

To that end, the NSF effort envisions the construction of a sprawling infrastructure that could cost approximately \$300 million. It would include research labs across the United States and perhaps link with research efforts abroad, where new architectures can be given a full workout. With a high-speed optical backbone and smart routers, this test bed would be far more elaborate and representative than the smaller, more limited test beds in use today. The idea is that new architectures would be battle tested with real-

world Internet traffic. "You hope that provides enough value added that people are slowly and selectively willing to switch, and maybe it gets enough traction that people will switch over," Parulkar says. But he acknowledges, "Ten years from now, how things play out is anyone's guess. It could be a parallel infrastructure that people could use for selective applications."

[[Click here](#) to view graphic representations of David D. Clark's four goals for a new Internet architecture.]

Still, skeptics claim that a smarter network could be even more complicated and thus failure-prone than the original bare-bones Internet. Conventional wisdom holds that the network should remain dumb, but that the smart devices at its ends should become smarter. "I'm not happy with the current state of affairs. I'm not happy with spam; I'm not happy with the amount of vulnerability to various forms of attack," says Vinton Cerf, one of the inventors of the Internet's basic protocols, who recently joined Google with a job title created just for him: chief Internet evangelist. "I do want to distinguish that the primary vectors causing a lot of trouble are penetrating holes in operating systems. It's more like the operating systems don't protect themselves very well. An argument could be made, 'Why does the network have to do that?'"

According to Cerf, the more you ask the network to examine data -- to authenticate a person's identity, say, or search for viruses -- the less efficiently it will move the data around. "It's really hard to have a network-level thing do this stuff, which means you have to assemble the packets into something bigger and thus violate all the protocols," Cerf says. "That takes a heck of a lot of resources." Still, Cerf sees value in the new NSF initiative. "If Dave Clark...sees some notions and ideas that would be dramatically better than what we have, I think that's important and healthy," Cerf says. "I sort of wonder about something, though. The collapse of the Net, or a major security disaster, has been predicted for a decade now." And of course no such disaster has occurred -- at least not by the time this issue of *Technology Review* went to press.

The NSF effort to make the medium smarter also runs up against the libertarian culture of the Internet, says Harvard's Zittrain. "The NSF program is a worthy one in the first instance because it begins with the premise that the current Net has outgrown some of its initial foundations and associated tenets," Zittrain says. "But there is a risk, too, that any attempt to rewrite the Net's technical constitution will be so much more fraught, so much more self-conscious of the nontechnical matters at stake, that the cure could be worse than the problem."

Still, Zittrain sees hazards ahead if some sensible action isn't taken. He posits that the Internet's security problems, and the theft of intellectual property, could produce a counterreaction that would amount to a clampdown on the medium -- everything from the tightening of software makers' control over their operating systems to security lockdowns by businesses. And of course, if a "digital Pearl Harbor" does occur, the federal government is liable to respond reflexively with heavy-handed reforms and controls. If such tightenings happen, Zittrain believes we're bound to get an Internet that is, in his words, "more secure -- and less interesting."

But what all sides agree on is that the Internet's perennial problems are getting worse, at the same time that society's dependence on it is deepening. Just a few years ago, the work of researchers like Peterson didn't garner wide interest outside the networking community. But these days, Clark and Peterson are giving briefings to Washington policymakers. "There is recognition that some of these problems are potentially quite serious. You could argue that they have always been there," Peterson says. "But there is a wider recognition in the highest level of the government that this is true. We are getting to the point where we are briefing people in the president's Office of Science and Technology Policy. I specifically did, and other people are doing that as well. As far as I know, that's pretty new."

Outside the door to Clark's office at MIT, a nametag placed by a prankster colleague announces it to be the office of Albus Dumbledore -- the wise headmaster of the Hogwarts School of Witchcraft and Wizardry, a central figure in the Harry Potter books. But while Clark in earlier years may have wrought some magic, helping transform the original Internet protocols into a robust communications technology that changed the world, he no longer has much control over what happens next.

But "because we don't have power, there is a greater chance that we will be left alone to try," he says. And so Clark, like Dumbledore, clucks over new generations of technical wizards. "My goal in calling for a fresh design is to free our minds from the current constraints, so we can envision a different future," he says. "The reason I stress this is that the Internet is so big, and so successful, that it seems like a fool's errand to send someone off to invent a different one." Whether the end result is a whole new architecture -- or just an effective set of changes to the existing one -- may not matter in the end. Given how entrenched the Internet is, the effort will have succeeded, he says, if it at least gets the research community working toward common goals, and helps "impose creep in the right direction."

Foundations for a New Infrastructure

The NSF's emerging effort to forge a clean-slate Internet architecture will draw on a wide body of existing research. Below is a sampling of major efforts aimed at improving everything from security to wireless communications.

PLANETLAB

Princeton University

Princeton, NJ

Focus: Creating an Internet "overlay network" of hardware and software—currently 630 machines in 25 countries—that performs functions ranging from searching for worms to optimizing traffic.

EMULAB

University of Utah

Salt Lake City, UT

Focus: A software and hardware test bed that provides researchers a simple, practical way to emulate the Internet for a wide variety of research goals.

DETER/University of Southern

California Information Sciences Institute

Marina del Rey, CA

Focus: A research test bed where researchers can safely launch simulated cyber--attacks, analyze them, and develop defensive strategies, especially for critical infrastructure.

WINLAB (Wireless Information Network Laboratory)

Rutgers University

New Brunswick, NJ

Focus: Develops wireless networking architectures and protocols, aimed at deploying the mobile Internet. Performs research on everything from high-speed modems to spectrum management.

Copyright Technology Review 2005.