

Thursday, December 01, 2005

The Internet Is Broken

The Net's basic flaws cost firms billions, impede innovation, and threaten national security. It's time for a clean-slate approach, says MIT's David D. Clark.

By David Talbot

This article -- the cover story in Technology Review's December 2005/January 2006 print issue -- has been divided into three parts for presentation online. This is [part 1](#); [part 2](#) will appear on Tuesday, December 20, and [part 3](#) on Wednesday, December 21.

In his office within the gleaming-stainless-steel and orange-brick jumble of MIT's Stata Center, Internet elder statesman and onetime chief protocol architect David D. Clark prints out an old PowerPoint talk. Dated July 1992, it ranges over technical issues like domain naming and scalability. But in one slide, Clark points to the Internet's dark side: its lack of built-in security.

In others, he observes that sometimes the worst disasters are caused not by sudden events but by slow, incremental processes -- and that humans are good at ignoring problems. "Things get worse slowly. People adjust," Clark noted in his presentation. "The problem is assigning the correct degree of fear to distant elephants."

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

Today, Clark believes the elephants are upon us. Yes, the Internet has wrought wonders: e-commerce has flourished, and e-mail has become a ubiquitous means of communication. Almost one billion people now use the Internet, and critical industries like banking increasingly rely on it.

At the same time, the Internet's shortcomings have resulted in plunging security and a decreased ability to accommodate new technologies. "We are at an inflection point, a revolution point," Clark now argues. And he delivers a strikingly pessimistic assessment of where the Internet will end up without dramatic intervention. "We might just be at the point where the utility of the Internet stalls -- and perhaps turns downward."

Indeed, for the average user, the Internet these days all too often resembles New York's Times Square in the 1980s. It was exciting and vibrant, but you made sure to keep your head down, lest you be offered drugs, robbed, or harangued by the insane. Times Square has been cleaned up, but the Internet keeps getting worse, both at the user's level, and -- in the view of Clark and others -- deep within its architecture.

Over the years, as Internet applications proliferated -- wireless devices, peer-to-peer file-sharing, telephony -- companies and network engineers came up with ingenious and expedient patches, plugs, and workarounds. The result is that the originally simple communications technology has become a complex and convoluted affair. For all of the Internet's wonders, it is also difficult to manage and more fragile with each passing day.

That's why Clark argues that it's time to rethink the Internet's basic architecture, to potentially start over with a fresh design -- and equally important, with a plausible strategy for proving the design's viability, so that it stands a chance of implementation. "It's not as if there is some killer technology at the protocol or network level that we somehow failed to include," says Clark. "We need to take all the technologies we already know and fit them together so that we get a different overall system. This is not about building a technology innovation that changes the world but about architecture -- pulling the pieces together in a different way to achieve high-level objectives."

Just such an approach is now gaining momentum, spurred on by the National Science Foundation. NSF managers are working to forge a five-to-seven-year plan estimated to cost \$200 million to \$300 million in research funding to develop clean-slate architectures that provide security, accommodate new technologies, and are easier to manage.

They also hope to develop an infrastructure that can be used to prove that the new system is really better than the current one. "If we succeed in what we are trying to do, this is bigger than anything we, as a research community, have done in computer science so far," says Guru Parulkar, an NSF program manager involved with the effort. "In terms of its mission and vision, it is a very big deal. But now we are just at the beginning. It has the potential to change the game. It could take it to the next level in realizing what the Internet could be that has not been possible because of the challenges and problems."

Firewall Nation

When AOL updates its software, the new version bears a number: 7.0, 8.0, 9.0. The

most recent version is called AOL 9.0 Security Edition. These days, improving the utility of the Internet is not so much about delivering the latest cool application; it's about survival.

In August, IBM released a study reporting that "virus-laden e-mails and criminal driven security attacks" leapt by 50 percent in the first half of 2005, with government and the financial-services, manufacturing, and health-care industries in the crosshairs. In July, the Pew Internet and American Life Project reported that 43 percent of U.S. Internet users -- 59 million adults -- reported having spyware or adware on their computers, thanks merely to visiting websites. (In many cases, they learned this from the sudden proliferation of error messages or freeze-ups.) Fully 91 percent had adopted some defensive behavior -- avoiding certain kinds of websites, say, or not downloading software. "Go to a neighborhood bar, and people are talking about firewalls. That was just not true three years ago," says Susannah Fox, associate director of the Pew project.

Then there is spam. One leading online security company, Symantec, says that between July 1 and December 31, 2004, spam surged 77 percent at companies that Symantec monitored. The raw numbers are staggering: weekly spam totals on average rose from 800 million to more than 1.2 billion messages, and 60 percent of all e-mail was spam, according to Symantec.

But perhaps most menacing of all are "botnets" -- collections of computers hijacked by hackers to do remote-control tasks like sending spam or attacking websites. This kind of wholesale hijacking -- made more potent by wide adoption of always-on broadband connections -- has spawned hard-core crime: digital extortion. Hackers are threatening destructive attacks against companies that don't meet their financial demands. According to a study by a Carnegie Mellon University researcher, 17 of 100 companies surveyed had been threatened with such attacks.

Simply put, the Internet has no inherent security architecture -- nothing to stop viruses or spam or anything else. Protections like firewalls and antispam software are add-ons, security patches in a digital arms race.

The President's Information Technology Advisory Committee, a group stocked with a who's who of infotech CEOs and academic researchers, says the situation is bad and getting worse. "Today, the threat clearly is growing," the council wrote in a report issued in early 2005. "Most indicators and studies of the frequency, impact, scope, and cost of cyber security incidents -- among both organizations and individuals -- point to continuously increasing levels and varieties of attacks."

And we haven't even seen a real act of cyberterror, the "digital Pearl Harbor" memorably predicted by former White House counterterrorism czar Richard Clarke in 2000 (see "[A Tangle of Wires](#)"). Consider the nation's electrical grid: it relies on continuous network-based communications between power plants and grid managers to maintain a balance between production and demand. A well-placed attack could trigger a costly blackout that would cripple part of the country.

The conclusion of the advisory council's report could not have been starker: "The IT infrastructure is highly vulnerable to premeditated attacks with potentially catastrophic effects."

The system functions as well as it does only because of "the forbearance of the virus authors themselves," says Jonathan Zittrain, who cofounded the Berkman Center for Internet and Society at Harvard Law School and holds the Chair in Internet Governance and Regulation at the University of Oxford. "With one or two additional lines of code...the viruses could wipe their hosts' hard drives clean or quietly insinuate false data into spreadsheets or documents. Take any of the top ten viruses and add a bit of poison to them, and most of the world wakes up on a Tuesday morning unable to surf the Net -- or finding much less there if it can."

In [Part 2](#): Why patching up the Internet with layers of security software isn't working - and what a safer new architecture might look like.

Copyright Technology Review 2005.