

WIRED.GOV

Single-window sensitivities

by Richard Bray

Forget Y2K. That's yesterday's news. The new and nasty flavour of the month is denial of service, or the "Big Hack Attack."

The next generation of electronic procurement tools are now being designed in the context of a federal network that may be highly centralized. Unfortunately, if recent experience with help desks and 1-800 numbers is any guide, the single point of access is a good way to stay in touch with elevator music but has little to do with swift and efficient customer service.

The move is also predicated on the belief that the general public is either incapable of finding, or unwilling to look for, their information at the department or branch level. If the assumption is that the general public lacks the skills to find specific websites, then how can we assume they have the skills to fill out the forms and manipulate the information they find on those sites?

Briefly, in the Big Hack Attack, a person or persons used programs and information – freely available on the Internet – to close down major websites. Apparently, they secretly planted programs on as many as 50 “innocent” computers around the world and then aimed a torrent of data at their targets. In effect, the sites were overwhelmed.

From all accounts, it appears that senior managers at the Internet's biggest superstars ignored basic security precautions in the rush to set up shop on the information highway. It's not as if Yahoo!, Buy.com, eBay or Amazon didn't have the money to install the software and hardware necessary to withstand the electronic assault. In the rush to cast the net where it would catch the gold, they simply did not take the time to guard against denial of service attacks. They certainly had enough warning. One security consultant said he has been raising the possibility of such an assault with clients for more than five years.

There is a second line of guilt in the February attacks on commercial Internet sites. By failing to install or maintain the necessary safeguards, network administrators around the world allowed their computers to be “recruited.” Suspicion fell on university and college systems first, because of their openness, but there can be little doubt that every kind of organization and institution could be implicated in the attacks. Hackers made the attacks happen. The people responsible for securing these computers allowed the attacks to happen.

And there is yet a third level of complicity in the situation and that is the various websites around the world that tolerate the storage and dissemination of dangerous software and documentation. There is nothing wrong with a spirited exchange of alternative viewpoints but that does not include handing out Molotov cocktails to every disaffected teenager with a modem.

The attacks have pointed out what appears to be a basic and dangerous instability throughout the Internet, but there is another assumption that needs to be questioned. For the people designing electronic government systems today, there may be great significance to the fact that each attack was directed at a single point – the individual Internet address. The denial of service attacks targeted the “brands” themselves. In the Internet age, www.yahoo.com is both the symbol and the substance. If you can damage one, you can damage both.

“Single point of access” or “one window” has the virtue of simplicity. Directing all incoming traffic to one single destination only *sounds* like a good idea if there is no “back office” to support the load. What happens to routine procurement functions, and everything else, if every last-minute taxpayer in the country files a return through the single point of access at the same time?

Remember testing the Christmas tree lights? It only took one bad bulb to black out the entire string. The lesson could hardly be clearer. When a network’s very survival depends on the integrity and efficiency of a single point, then that network has a significantly higher risk of failure.

There are probably many lessons in the denial of service attacks. Don’t ignore the obvious threats. Never underestimate the nerve of a teenage hacker. Guard against the malice of a disaffected employee. And make sure the network can work around a burnt-out bulb.

[Richard Bray](#) is a freelance writer based in Nepean, Ontario, specializing in Canada’s high technology sector. His work has appeared in magazines and newspapers in Australia, the US and Canada. He has worked as a producer, reporter and senior news editor with the CBC in Toronto.