

"Old" Internet flaw persists

By Peter Svensson, Associated Press - May 9, 2010

In 1998, a hacker told Congress that he could bring down the Internet in 30 minutes by exploiting a certain flaw that sometimes caused online outages by misdirecting data. In 2003, the administration of President George W. Bush concluded that fixing this flaw was in the nation's "vital interest."

Fast forward to 2010, and very little has happened to improve the situation. The flaw still causes outages every year. Although most of the outages are innocent and fixed quickly, the problem still could be exploited by a hacker to spy on data traffic or take down websites. Meanwhile, our reliance on the Internet has only increased. The next outage, accidental or malicious, could disrupt businesses, the government or anyone who needs the Internet to run normally.

The outages are caused by the somewhat haphazard way that traffic is passed between companies that carry Internet data. The outages are called "hijackings," even though most of them are not caused by criminals bent on destruction. Instead the outages are a problem borne out of the open nature of the Internet, a quality that also has stimulated the Net's dazzling growth.

"It's ugly when you look under the cover," says Earl Zmijewski, a general manager at Renesys Corp., which tracks the performance of data routes. "It amazes me every day when I get into work and find it's working."

When you send an e-mail, view a Web page or do anything else online, the information you read and transmit is handed from one carrier of Internet data to another, sometimes in a long chain. When you log into Facebook, your data might be handed from your Internet service provider to a company such as Level 3 Communications Inc., which operates a global network of fiber-optic lines that carry Internet data across long distances. It, in turn, might pass the data to a carrier that's connected to Facebook's servers.

The crux of the problem is that each carrier along the way figures out how to route the data based only on what the surrounding carriers in the chain say, rather than by looking at the whole path. It's as if a driver had to get from Philadelphia to Pittsburgh without a map, navigating solely by traffic signs he encountered along the way — but the signs weren't put up by a central authority. If a sign pointed in the wrong direction, that driver would get lost.

That's essentially what happens when an Internet route gets hijacked. Because carriers pass information between themselves about where data should go — and this system has no secure, automatic means of verifying that the routing information is correct — data can be routed to some carrier that isn't expecting the information. The carrier doesn't know what to do with it, and usually just drops it. It falls into a "black hole."

On April 25, 1997, millions of people in North America lost access to the Internet for about an hour. The hijacking was caused by an employee misprogramming a router, a computer that directs data traffic, at a small Internet service provider.

A similar incident happened elsewhere the next year, and the one after that. Routing errors also blocked Internet access in different parts of the world, often for millions of people, in 2001, 2004, 2005, 2006, 2008 and 2009. Last month a Chinese Internet service provider halted access from around the world to a vast number of sites, including Dell.com and CNN.com, for about 20 minutes.

In 2008, Pakistan Telecom tried to comply with a government order to prevent access to YouTube from the country and intentionally "black-holed" requests for YouTube videos from Pakistani Internet users. But it also accidentally told the international carrier upstream from it that "I'm the best route to YouTube, so send all YouTube traffic to me." The upstream carrier accepted the message, and passed it along to other carriers across the world, which started sending all requests for YouTube videos to Pakistan Telecom. Soon, even Internet users in the U.S. were deprived of videos of singing cats and skateboarding dogs for hours.

In 2004, the flaw was put to malicious use when someone got a computer in Malaysia to tell Internet service providers that it was part of Yahoo Inc. A flood of spam was sent out, appearing to come from Yahoo.

"Hijacking is very much like identity theft. Someone in the world claims to be you," said Todd Underwood, who worked for Renesys during the Pakistan Telecom hijacking. He now works for Google Inc., trying to prevent hijacking of its websites, which include YouTube.

In 2003, the Bush administration's Critical Infrastructure Protection Board assembled a "National Strategy to Secure Cyberspace" that concluded that it was vital to fix the routing system and make sure the "traffic signs" always point in the right direction.

But unlike Internet bugs that get discovered and fixed relatively quickly, the routing system has been unreformed for more than a decade. And while there's some progress being made, there's little industry-wide momentum behind efforts to introduce a permanent remedy. Data carriers regard the fallibility of the routing system as the price to be paid for the Internet's open, flexible structure. The simplicity of the routing system makes it easy for service providers to connect, a quality that has probably helped the explosive growth of the Internet.

That growth has also increased the risks exponentially. Fifteen years ago, maybe 8,000 people in the world had access to computers that use the Border Gateway Protocol, or BGP, which defines how carriers pass routing information to each other. Now, Danny McPherson, chief security officer at Arbor Networks, believes that with the growth of Internet access across the world and the increase in the number of carriers, that figure is closer to 1 million people.

Peiter Zatk0, a member of the "hacker think tank" called the L0pht, told Congress in 1998 that he could use the BGP vulnerability to bring down the Internet in half an hour. In recent years, Zatk0 — who now works for the Pentagon's Defense Advanced Research Projects Agency — has said the exploit would still work. However, it would likely take a few hours rather than 30 minutes, partly because a greater number of carriers would need to be hit.

Plenty of solutions have been proposed in the Internet engineering community, going back as far as 1995. The U.S. government has supported these efforts, spurred in part by the Bush administration's 2003 statement. That has resulted in some trials of new technology, but adoption by carriers still appears distant. And the government doesn't have any direct authority to force changes.

One reason is that the weaknesses are in the routing between carriers. It doesn't help if one carrier introduces a new system — every one it connects with has to make the change as well. "It's kind of everybody's problem, because it impacts the stability of the Internet, but at the same time it's nobody's problem because nobody owns it," says Doug Maughan, at the Department of Homeland Security.

Pieter Poll, the chief technology officer at Qwest Communications, says he would support some simple mechanisms to validate data routes, but he argues that fundamental reform isn't necessary. Hijackings are typically corrected quickly enough that they don't pose a major threat, he argues.

One fix being tested would stop short of making the routing system fully secure but would at least verify part of it. Yet this system also worries carriers because they would have to work through a central database.

"My fear is that innovation on the Internet would slow down if there's a need to go through a central authority," Poll says.

Jeffrey Hunker, a former senior director for critical infrastructure in the Clinton administration, says he's not surprised that little has happened on the issue since 2003. **He doesn't expect much to happen in the next seven years, either.**

"The only thing that's going to drive adoption is a major incident, which we haven't had yet," he says. "But there's plenty of evidence out there that a major incident would be possible."

In the meantime, network administrators deal with hijacking an old-fashioned way: calling their counterparts close to where the hijacking is happening to get them to manually change data routes. **Because e-mails may not arrive if a route has been hijacked, the phone is a more reliable option,** says Tom Daly, chief technical officer of Dynamic Network Services Inc., which provides Web hosting and other Internet services.

"You make some phone calls and hope and pray," Daly says.

STLtoday.com

<http://www.stltoday.com/stltoday/business/stories.nsf/story/EEB5A07B82E2B45E8625771D0011FA3D?OpenDocument>

© 2010 Associated Press. All Rights Reserved.