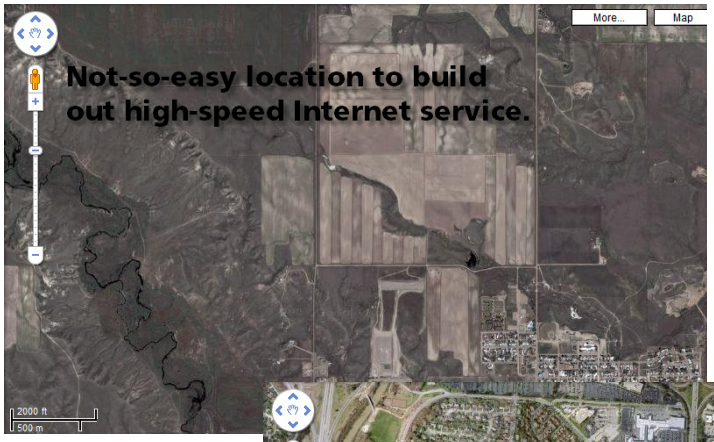
Random Thoughts
from William Blinn Communications
TECHNOLOGY • MARKETING • COMMUNICATIONS
April 2009

Why Is the Internet So Slow in the U.S.?

A recent account on the BBC noted that Virgin Media will beat British Telecom to the marketplace with 100Mbps broadband speeds. Virgin plans to start rolling out its fiber network next year and will complete the process by 2012. Until then, the Brits will have to make do with a top speed of 50Mbps. Make do? Every time I begin to feel good about my 6Mbps download speed, I run across a story about a service that's more than 8 times faster than what I have. In Japan, 60Mbps service is available today. And it costs about what I pay for far slower service. Why?



In part, it's because the Federal Communications Commission has, for nearly a decade, failed to do what it's supposed to do. Instead of promoting technology, the FCC was in a continuous tizzy about "dirty words" or "costume malfunctions". But that's not the sole cause of the problem. In part, it's because the United States is so large.

The *CIA Fact Book* lists the 5 largest countries in the world, by land mass: Russia, Canada, U.S., China, and Brazil. Sorting the list for the largest countries by population, a different picture emerges: China, India, U.S., Indonesia, and Brazil. Neither view provides a clear indication of why high-speed Internet and cellular service takes so long to build out in the United States.

It's the Density

The real story is population density and sorting the list that way produces a far different picture. This time I'll list the top 10 countries because a few in the top 10 are so small that they can be ignored for the purposes of this story: Macau, Monaco, Hong Kong, Singapore, Gibraltar, Malta, Bermuda, Maldives, Bahrain, and Bangladesh. On that list, the U.S. is number 175.

Take Hong Kong for example, third on the list. Hong Kong Broadband Network Limited reaches more than 90% of homes in Hong Kong and its slow speed is 25Mbps. Speeds up to 1000Mbps are available.

Clearly population density isn't the entire story. A poor nation with a high population density won't see high-speed Internet service anytime soon. But a reasonably prosperous nation that has a relatively high population density provides conditions that are ideal to support widespread high-speed service.

Fiber is costly to deploy and if the population density hovers around 2 people per square mile, as in Mongolia, there's little incentive to install fiber. On the other hand, Taiwan (600+ people per square mile), South Korea (490), Japan (336), Great Britain and Germany (each around 240), and Switzerland (180) have the investment capital and the population density to support a fast build-out.

China is 76th with a density of just over 130 people per square mile compared to the U.S. with a density less than 30. It's true that about 80% of us live in metro areas, though, and it's unlikely that someone who lives on Beer

If you'd like to see the spreadsheet I used to compare population, land mass, and density, let me know and I'll send you the document.

Random Thoughts (ISSN 1543-1533) is for clients and friends of William Blinn Communications, 179 Caren Avenue, Worthington, Ohio 43085. Phone 614.785.9359. On the Web at www.Blinn.com.

"A cat is *always* on the wrong side of the door."

Can Alley, about 5 miles north of Wolf Point, Montana, expect high-speed service anytime soon.

The Solution for Beer Can Alley

If you live in northeast Montana (or just about anywhere else in the country) you can have "high-speed" Internet access if you're willing to pay. HughesNet Satellite has 6 tiers of service:

- Home - 1.0 Mbps downstream / 128 Kbps upstream / $60 monthly: That's about 20 times the speed of a modem connection for about 3 times the cost of modem service.
- Pro - 1.2 Mbps down / 200 Kbps up / $70 monthly.
- ProPlus - 1.6 Mbps down / 250 Kbps Up / $80 monthly: These two services provide a slight increase in the downlink speed, but the primary advantage is the faster uplink, which is helpful if you need to upload files.
- Elite - 2.0 Mbps down / 300 Kbps up / $120 monthly.
- ElitePlus - 3.0 Mbps down / 300 Kbps up / $190 monthly.
- ElitePremium - 5.0 Mbps down / 300 Kbps up / $350 Monthly: These are speeds that a cable or DSL subscriber would pay $40 to $60 per month for.

No Easy Solutions

For those who live in or near to cities, where houses are close together, fiber could be built out relatively fast. In many cases, fiber is already in the neighborhood. All that's needed is the time, money, and effort required to run fiber from a utility pole to and through your home.

As for the guy who waiting for high-speed service on Beer Can Alley: Don't hold your breath. ß

Browsers Vulnerable

Find a browser bug and collect $5000. That's the basis of a contest held recently by CanSecWest in Vancouver. CanSecWest is a security conference in, well, the western part of Canada. This was the 10th annual conference and it's billed as "the world's most advanced conference focusing on applied digital security." The conference included a "Pwn2Own" contest. That would be leet-speak for "own to own": If you write an exploit that "owns" the machine, you earn $5000 and you own the laptop computer used for the contest.

The winner was a German guy known only as "Nils". He presented 3 new exploits, 1 each for Firefox, Safari, and Internet Explorer.

Ease of use is paramount for a browser and, because of that, security sometimes must sit in the back seat. But even if security was paramount, there would still be flaws because programmers write imperfect programs and because browsers are exposed on the Internet for every crook in the world to play with.

You might think a conference such as CanSecWest, which brings hackers together to compare notes, is a bad thing. It's not. The truly bad folks find security problems and share them. Conferences such as CanSecWest help to uncover security flaws and then report those flaws to the vendor. In Microsoft's case, the flaw that Nils revealed was patched the next day when Microsoft released the first non-beta version of the browser.

Nils took home the Sony Vaio notebook used at the conference, along with $5000 each for the flaws he demonstrated in Safari, IE, and Firefox.

The hacker, a student at a German university, didn't release his last name because he wanted to avoid being sought out by criminals who would want to buy information about his exploits. He did explain, though, that he found it a lot easier to write the exploit for Firefox or Safari on the Mac's OS X than on Windows Vista.

Yes, you did read that correctly: Vista was significantly more secure than OS X. Nils says that he expects more exploits to be written specifically for the Mac as Windows users migrate to Vista or (more likely) to Windows 7 when that version of the operating system is released.

A word to the Mac wise: You have been warned. ß

World Ends! (Again.)

Based on what's been written on some blogs and in the "old media", too, a botnet that takes over some routers spells the end of the Internet as we know it. Drone Blacklist has been on the receiving end of distributed denial-of-service attacks from these corrupted routers and it's the company that announced the presence of the router-borne botnet. Drone isn't particularly concerned about the threat, though, and says that the botnet seems to have been taken out of service.

When every possible exploit becomes "the end of the Internet as we know it", the noise level increases. When the noise level increases, legitimate messages are lost in the clutter. It's the Chicken-Little syndrome. Every time you hear that the sky is falling and then the sky doesn't fall, you become a bit less likely to pay attention to the next warning.

I sincerely wish that those who write about technology (and that includes SlashDot) would be a bit more careful about what they write.

As Drone Blacklist describes the problem on its website, your router would be vulnerable only if it's a *mipsel* device (MIPS running in little-endian mode), if it presents an SSH or Web-based interface to the WAN, and if you have a weak user name and password or the firmware is exploitable.

In short, "90% of the routers and modems participating in this botnet are participating due to user-error (the user themselves or otherwise). Unfortunately, it seems that some of the people covering this botnet do not understand this point, and it is making us look like a bunch of idiots."

Those devices that have been compromised can be easily disinfected: "[S]imply power cycle your device and take appropriate action to lock it down, including the latest firmware updates, and using a secure password."

There, now. That wasn't so bad, was it? ß