

Dan Kaminsky
Director Of Penetration Testing
IOActive, Inc.
1401 Boren Ave. #908
Seattle, WA, 98101
(408) 933-8195

Esteemed Colleagues,

Thank you for the opportunity to comment upon the nature of Network Neutrality. I write to you as a researcher, a developer, and a creator of large scale, high speed, network analysis software. I am also a security researcher of some repute; I've spent the last seven years speaking at the Black Hat Briefings, a noted security conference. I have spent the last year and a half embedded within Microsoft, consulting with them to secure their upcoming operating systems. Finally, I was directly involved with tracking down the scale of Sony's "rootkit", a widely distributed instance of malicious software, using a large scale network scanning technique of my own design.

You have, I'm sure, heard many arguments for and against the enforcement of neutral prioritization of traffic flows. Some time ago, I wrote an article on this very subject, but I looked at it from the perspective of a developer who will be working to bypass the neutrality blocks the end providers propose. I won't restate the entire article, but here's a few key points to keep in mind:

- 1) The neutral Internet will continue to exist, because there is sufficient competition at the core to prevent any provider from going deeply non-neutral. That means, everyone is only a few hops away from a real, neutral network link.
- 2) To acquire the non-neutral punishment the end providers seek, they must suppress connections to non-neutral drops. **Since these links will inevitably be encrypted, any non-neutral network will penalize encrypted traffic. This will directly increase identity theft on the Internet.**
- 3) There is direct precedent for end providers cutting off access to encrypted channels. Here, in its entirety, is an email sent by ComCast, sourced from <http://www.practicallynetworked.com/news/comcast.htm> :

Thank you for your message.

The Comcast @Home product is, and has always been, designated as a residential service and does not allow the use of commercial applications. A VPN or Virtual Private Network is primarily used to connect Internet users to her or his work LAN from an Internet access point.

High traffic telecommuting while utilizing a VPN can adversely affect the condition of the network while disrupting the connection of our regular residential subscribers.

To accommodate the needs of our customers who do choose to operate VPN, Comcast offers the Comcast @Home Professional product. @Home Pro is designed to meet the needs of the ever growing population of small office/home office customers and telecommuters that need to take advantage of protocols such as VPN. This product will cost \$95 per month, and afford you with standards which differ from the standard residential product.

If you're interested in upgrading your current Comcast @Home service to Comcast @Home Pro, please e-mail your name, address, and phone number to: sales@comcastpc.com. Prior to Sept 15th, you will be contacted by one of our Comcast

@Home Pro representatives to discuss upgrading from your current Comcast @Home residential service.

While VPN is not a prohibited use of the @Home Pro product, Comcast does not provide support for VPN technology. All inquiries regarding VPN should be directed toward your company's network administrator.

Currently, the Comcast @Work commercial services do provide VPN support. If your company pays for your internet service, or if you would like to use supported VPN or IP tunneling, please contact our commercial services at 888-638-4338 or visit www.comcastwork.com.

If there is anything else we can help you with, please contact us. Thank you for choosing Comcast@Home.

*Steve
Comcast@Home
Email Response Specialist*

"Internet Isolationism", as I've been referring to it, puts both telecommuters and consumer identities at risk. I request your assistance, and offer my own, to protect American consumers and small businesses from having their private communications held hostage.

I attach now an article I wrote on this subject. Thank you for your time!

What if you had to pay to receive packages from FedEx?

Oh, sure, there's UPS and DHL and the US Postal Service. But imagine if they were all proposing that, because people make money based on the contents of packages other people shipped, that they should see some of that money. Imagine they implied that, if you or your company did not pay a reception fee... well, things might happen. Packages might get lost, you see.

Now imagine they informed you that they were going to deploy equipment that could analyze the contents of the packages they shipped. A six-ounce letter might contain a multimillion dollar contract, while a twenty pound box might just have some intern's new laptop. Suppose their equipment could tell the difference. Would you pay to not have that contract "lost" in a sorting facility?

Of course you'd pay. You'd also pay not to have your knees broken. But kneecap integrity should not be a business expense.

This is, of course, a simplification. Nowadays, that contract could be transmitted over the Internet instead, and work would continue to flow. But something very strange has been proposed for the Net: Broadband providers have suggested that, like FedEx charging to receive packages, certain receivers should have to pay to receive packets. Though they've been coy about what it would mean to not pay, broadband providers have indeed proposed deploying an entire network of monitoring and censoring agents that could examine network traffic and suppress it, unless a "business arrangement" had been made with the receiving parties.

FedEx would never suggest intentionally losing your packages. They also would never suggest tearing them open to see if there's anything good inside. But Verizon and Comcast and a number of other broadband providers are gleefully declaring their intent to drop your traffic, starting with whatever you consider most valuable. This, they call "innovation".

We've got a problem here.

The status quo on the Internet is something referred to as network neutrality. This basic idea -- that it's the Internet's job to move data, not to inspect and select and ultimately reject it -- has worked quite well. What one particular branch of the Internet is suggesting is something rather different: Internet isolationism. They wish to redefine their customers as a "captive audience", suppressing the free trade of packets to them unless as-yet undefined tariffs are paid. They propose to isolate their customers behind an ever-shifting web of favored providers, special partners, and mutually beneficial arrangements.

This was, of course, the model of both America Online and France's Minitel. Neither model came close to the success of the Internet.

The broadband providers have said this is about creating a faster Internet -- one that can move video faster. But if this was what the providers wanted, why not deploy reliable multicast technology, which is actually designed to allow millions of users to efficiently consume video, next-generation games, and security patches? They've said this is about allowing web sites to compete. Imagine if China's Baidu paid dearly to be the only search engine that could be accessed in America at broadband rates. Can anyone imagine the trade war at WTO that would erupt? This is a red herring, not worthy of even a moment's consideration. No, these efforts must be about something else entirely.

Internet Isolationism is actually about holding telecommuters ransom from the companies that employ them. According to Broadband Week, the size of the U.S. telecommuting market was 40 million people -- in 2004. As commutes increase and oil becomes scarcer, the ability for knowledge workers to have full access to corporate resources no matter where they happen to be is critical to the success of American business. If telecommunications providers could extract just \$100 more a year -- under \$10 a month! -- from each of the 40 million users, that'd be four billion dollars of additional revenue, per year.

Would you pay a quarter to check your work email from home? Would your office pay a quarter to make sure you could? Broadband providers want that quarter, and have essentially stated they'll alter and degrade the network more and more until they get it. But why do they deserve that quarter? They're not the only provider that's involved with getting a packet from home to work; they're just the branch with the least competition. This is a logistical artifact -- only a couple broadband providers can physically serve each region. In this regard, they're like airports. You might have dozens of airlines, but only a few runways on which they can land.

Imagine for a moment that salespeople had to give a chunk of their commission to the airport they flew out of, and you'd have an idea of why the Internet community is horrified by Internet isolationism.

It gets worse. According to something known as Metcalfe's Law, the value of a network increases substantially with the number of other people you can connect to. On isolated networks, your connectivity is reduced, and therefore the value of your link plummets. But the real Internet is still out there; there's just a "fog bank" placed in front of it by your broadband provider. Therefore, the first thing you do when connecting to the Internet is to escape your broadband provider and get to "network neutral territory". This involves setting up a session, probably encrypted, and making your way out to a node that will give you genuine access to the Internet.

Citizens of countries outside the United States are quite familiar with the need to find "proxies" with greater freedom than their state providers are willing to provide. Imagine if Americans needed to live under the same restrictions!

Consider the proxy problem from the broadband provider side, though. You want to create an isolated network, where non-payment of access fees by a receiver leads to suppressed access for a telecommuting employee. You have to thus suppress any mechanism by which traffic can escape your network that has not gone through the correct toll check. As a security engineer, I am deeply concerned about anything that would make it more difficult for businesses and organizations to deploy secure systems. If the underlying network actively discourages encrypted communication, communication will simply not be encrypted -- to the delight of identity thieves everywhere. I also find myself concerned about the geopolitical implications of making

telecommuting more difficult: With depressed oil stocks, is now the best time to be throwing into question whether the network will be there for telecommuters to operate? It sure looks like regions that enforce neutral broadband will have quite the advantage over those suffer the yoke of isolation.

We can do better than what Internet isolationism suggests. In fact, we *have* done better. Net neutrality has been the "secret sauce" behind a decade of business transformation. The simple fact that negotiations between two businesses can be conducted over email, without any special networking arrangements made beforehand, was something that simply could not happen under previous circumstances. But today, inter-company email is something we just take for granted -- something made possible, of course, by network neutrality. Broadband providers suggest we abandon this status quo for a radical philosophical departure that has failed everywhere else it has been tried. They suggest Internet isolationism, and they do so not just at their peril, but at ours.