CircleID™
THE INTERNET ADDRESSING NETWORK

Home | Subscribe | Archives | Submit | About | Contact | Feedback

SUBSCRIBE
CircleID Newsletter

Previous Articles

Tell A Colleague

SPONSORS

UltraDNS
NetNation
DomainPeople

Email This Article | Subscribe To CircleID | Read Feedback

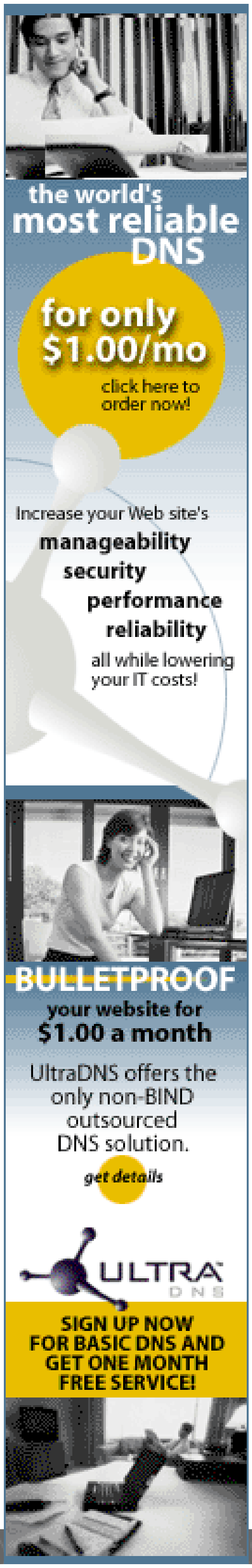
IPv6: In Search Of Internet Security

October 9, 2002 | By Joe Baptista | Article Feedback

My recent articles on IPv6 published this past September 12 and 25 have left many users with the impression that IPv6 (Internet Protocol version 6) is secure. This is a false assumption. Internet security is more an act of faith in a complex science draped in a religious mystery - in other words non-existent. In my opinion, Internet security has never existed. Any protocol can be violated. IPv6 has the power to make users' communication more secure during transmission. It also can be a security nightmare. So be warned, users of IPv6 - it will bypass your firewall settings but it will give your users enhanced privacy. But the experts are working on it.

To understand Internet security it's always a good idea to go back in history. The Internet was a military sponsored communication project developed under DARPA (The Defense Advanced Research Projects Agency). The idea at the time was to distribute computer resources by decentralizing control and increasing redundancy on United States military and government networks. The goal was to prevent a first strike from taking out computational and communication facilities essential to operations. If the red menace (Soviet Union) bombed a computer facility in Kansas the network would route around the damage and survive.

DARPA planners unfortunately were short sighted and did not anticipate the technology would become an international standard for communications. The community of users and networks connected to DARPA were small and trusted so security concerns were a low priority. The end result was the deployment of insecure



protocols that have kept many security experts gainfully employed. Even secure protocols are hacked. Today there are millions of compromised computer systems busy trying to hack other computers. And many of those busy hacking computers may no longer be under the control of the original script kiddy hacker who launched them. In fact I suspect many such computers are operating independently of a human operator.

IPv6 does fix a lot of the privacy issues and has some added security features that make it a better transport. Keith Moore, a researcher with the computer science department at the University of Tennessee, points out that "security is not an IPv6 issue any more than it is an IPv4 issue - probably slightly less." Moore, a former applications area director to the Internet Engineering Steering Group, points out that users of IPv6 will have an added advantage over IPv4. IPv6 transports traffic using the IPsec security protocol.

IPv4 connections move traffic around in the clear (plain text). It is up to the user to ensure traffic is encrypted. Sniffer programs at various Internet exchange points can easily intercept most user web and email traffic. Cable users sometimes install sniffer programs to monitor and record IPv4 transmissions. In most cases they don't have the means to decrypt security protocols and they do it mostly for the fun and entertainment value. So don't panic, your credit card is still confidential provided you used it over a secure web session. However don't expect to send your credit card data to Uncle Steve via email. If you have however emailed confidential information to someone chances are your message was transported as plain text and can be subject to interception.

The industry would agree that IPv4 is a brain dead protocol and those predicting it's death have good reasons for their position. Government programs like carnivore depended on IPv4 vulnerabilities to be successful. Carnivore is a tool that has revitalized worldwide respect for the FBI in the intelligence community. The program intercepts and analyzes Internet traffic and is classified by the FBI as a diagnostic tool. Carnivore is also a motivating factor in the transition to IPv6 by American, European and Japanese governments.

Governments understand their vulnerabilities under IPv4; their intelligence departments have diagnostic tools too. IPsec makes IPv6 less prone to man in the middle interception or attacks. User data under IPv6 is encrypted across the transmission end points. Sure the intelligence establishment has the means to break encrypted protocols but that's an expensive affair. Carnivore has not been effective in catching terrorists who communicate using encrypted channels. But it's been very effective in catching child pornographers that have yet to discover the privacy features available to them under IPv6. It is easy to envision that Carnivore will become a useless diagnostic tool under the new protocol.

But in many cases IPv6 systems can be less secure. Your firewall may prevent access to your Microsoft shares under IPv4 but they will be wide open to IPv6 users. Iljitsch van Beijnum a freelance network specialist and author of "Border Gateway Protocol" the network routing howto manual has some concerns when it comes to security. Beijnum warns that many Unix boxes are heavily firewalled in IPv4 but not in IPv6. "If you happen to be on their local link (hello wireless)" said Beijnum "you can circumvent the IPv4 access restrictions for services that are v6-enabled". He explains that in most cases users don't even know the box is doing IPv6. User should secure their systems prior to turning on or installing IPv6 services.

On the brighter side of the IPv6 universe, workstations will be easier to hide from the evil hacker. An IPv6 allocation contains addresses in the trillions. This means old hacker tricks like scanning a network will become less affective. When your workstation uses one address out of trillions it makes targeted probes a less likely menace to an individual or organization. IPv6 workstations, which use privacy extensions for stateless address autoconfiguration, will certainly benefit. However systems which are using old IPv6 protocol stacks that do not incorporate the privacy extensions developed by Thomas Narten of IBM and Track Draves at Microsoft Research will most likely be targets for tracking. Old IPv6 protocols may publish your workstation or laptops unique electronic fingerprint. Make sure your IPv6 system is RFC 3041 compliant or else your privacy may be at risk.

Conclusion: IPv6 is a protocol that delivers on user privacy. If you want your enterprise servers to provide privacy to your facilities then IPv6 is the way to go. If you want security the best advise I can give any Internet user is that you pray and have faith or disconnect your computer when not in use. Enterprises, non-profit organizations, governments and small business that have a need for privacy should consider a transition to IPv6. But make sure you get a security check done on your systems. Those interested in connecting to the IPv6 network should visit the IPv6 forum and I maintain a list of providers. Enjoy!

Joe Baptista is a managing director of The dot.GOD Registry, Limited a not for profit provider of network infrastructure, and domain names inclusive namespace. Joe is also involved in Internet governance as a member of the General Assembly of the Domain Name Supporting Organization (DNSO) of The Internet Corporation for Assigned Names and Numbers (ICANN). Joe has been interviewed by the leading Canadian newspapers, radio and television on various Internet issues.

Home | Subscribe | Archives | Submission | About | Contact | Feedback

Interested in submitting your articles? Learn More
Please send us your Feedback & Error Reports. Thank You.