Internet Protocol Version 6: *Data Security and Privacy Concerns with the New Internet*

By Michael W. Hubbard

The implementation of IPv6 is important to the technological competitiveness of Europe. However whilst the rapid deployment of IPv6 should be encouraged, this should not be at the expense of safeguarding certain important principles.

—*IPv6: Legal Aspects of the New Internet Protocol* (Euro6IX 2005)

All organizations will need to develop security plans and policies for dealing with IPv6 traffic, regardless of their decisions whether and when to transition to IPv6.

These realities, coupled with the fact that bad actors are rapidly adopting IPv6 and are already using it to initiate attacks and hide malicious processes and communications, suggest that all organizations should develop explicit plans to provide, or prevent, IPv6 communications. Failure to do so will create the real potential that IPv6 will appear and be used on an organization network either by accident or for malicious intent.

—U.S. Department of Commerce, National Institute of Standards and Technology, National Telecommunications and Information Administration, *Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)* (January 2006)

Suppose that a manufacturer could instantly locate and track every item in stock in real time, whether the item was on a shelf in Beijing or a truck in Boston. Or imagine that, within seconds of a crash on the interstate, police and rescue crews already had critical information about the wreck and the vehicles involved. Or imagine that monitoring sensors on a bridge can communicate in real time with a bridge safety officer.

Such advances are right around the technological corner, thanks to Internet Protocol Version 6 (IPv6), the new language that allows devices to communicate via the Internet. IPv6 technology will allow for a more powerful, more flexible, and more portable Internet, from which businesses stand to reap great benefits.

But user privacy and data protection remain key concerns with respect to IPv6, just as they are with the current protocol version, IPv4. Protecting the privacy of Internet users is essential to the success of IPv6. Commentators on both sides of the Atlantic have raised concerns about privacy as it relates to implementation of the latest protocol.

IPv6 provides a near-limitless number of Web addresses. The change from 32-bit IP addresses to 128-bit IP addresses will allow the Internet—and internal networks—to be used in ways not currently possible.

One of the primary benefits of the Internet—the ability to transmit huge amounts of data around the world instantaneously—is also its major weakness when it comes to data protection. Vast amounts of information about Internet users are collected each day—sometimes without their knowledge or consent. As people conduct more and more of their business online, they are leaving a larger electronic footprint for would-be thieves to follow and ultimately raid. Viruses, Internet worms, spam, botnets, spoofing, and other forms of online attacks have so far proven a difficult problem to contain, and a conversion to IPv6 will introduce new challenges to ensuring user privacy and data security.

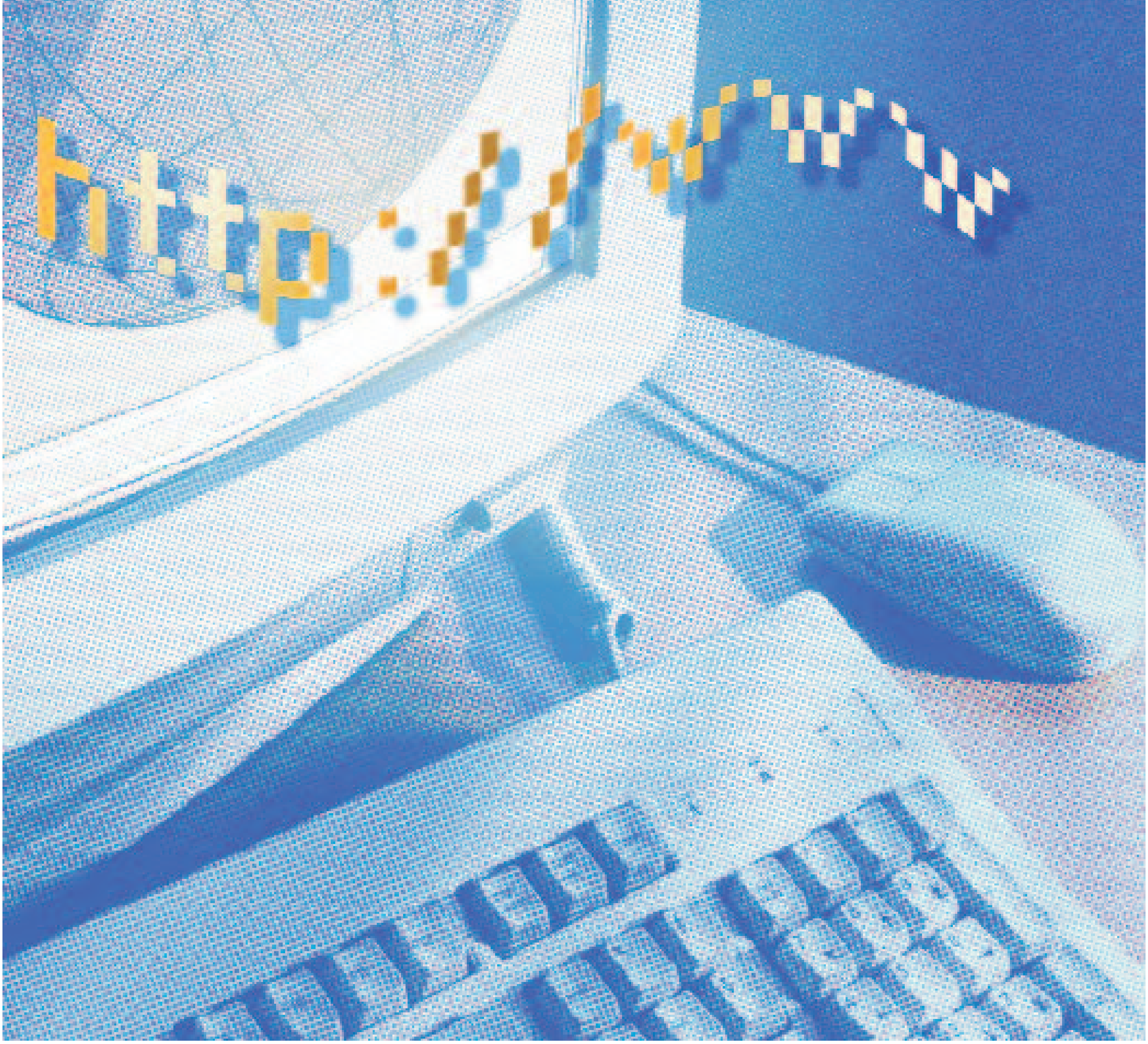
What Is IPv6 and How Will It Affect Businesses?

IPv6 is the latest edition of the platform that supports the entire Internet. The current version, IPv4 (IPv5 never got off the ground), has existed for 20 years and is considered by many to lack the capacity that businesses will demand in the future. Experts have been calling for a next-generation Internet Protocol since 1991.

That update is now here. All U.S. federal agencies must be IPv6-compliant by mid-2008. Given the number of companies that do business with the U.S. government, the federal mandate should lead to accelerated conversions in the commercial sector as well. And, as far as businesses are concerned, one of the greatest promises of IPv6 is the new platform's ability to provide a nearly limitless supply of Internet addresses.

To put things in perspective: IPv4 supports about 4.2 billion distinct Internet addresses—or fewer than one for every person on the planet. IPv6, on the other hand, supports 340 undecillion (that's 36 zeroes) addresses—more than enough to supply each grain of sand on the world's beaches with its own Internet address.

IPv6 is emerging at the same time as wireless broadband networks that necessitate an increase in IP addresses and greatly expand the practical applications for those IP



addresses. This new source of Internet addresses will enable an entire new generation of complex wireless devices, for example.

The possibilities and potential benefits of IPv6 are particularly staggering in the supply chain industry. Every package, parcel, and cargo crate could have its own unique Internet address, and wireless broadband technology will allow that address to be transmitted cheaply and easily. As a result, customers and shipping companies will be able to go online and instantly track their package to a precise location anywhere in the world, in much the same way as global positioning systems currently track vehicles on the highways. Through IPv6, these items can have their own routable Internet addresses without the need for any Internet server. This technology can vastly improve how companies track and ship cargo, providing both cost savings for companies and better service for customers.

IPv6 also has significant implications for businesses involved in the personal safety and homeland security industries. Specific information—a crash victim's medical records, for example—can be automatically collected and sent to the appropriate authorities using this new technology, similar to the way packages can be tracked when they are being shipped.

First responders such as firefighters and police departments will have faster and more reliable electronic communications with one another using an IPv6 rather than an IPv4 platform, because the "end-to-end" communications features of IPv6 are not available in IPv4. Recognizing this, the city of Harrisonburg, Va., has already implemented a municipal-wide IPv6 wireless network that substantially aids first responders in that community.

Some have speculated that an organization can obtain lower charges from its Internet service provider (ISP), because IPv6 will enable the organization to purchase fewer public Internet addresses from the ISP. Instead, the organization may use the additional addressing features of IPv6 to enable Internet communications to and from computers on the organization's internal network.

The U.S. government has set a June 30, 2008, deadline for all government agencies to be IPv6-compliant. Most federal agencies are not on track to meet that deadline, however. To date, the nation lacks a single organized effort to implement IPv6. Representing a significant step toward expanding IPv6 compliance in the United States, Microsoft will make its newest version of the Windows operating system IPv6-compliant.

The Slow Road to IPv6 Implementation

In the United States, the federal government is a leader in conversion to IPv6. Many expect the private sector will follow the government's lead, particularly those companies that have contracts with the U.S. government, the world's largest purchaser. But so far, the switch from IPv4 to IPv6 is going more slowly than originally anticipated, which makes it more difficult to assess the privacy and data security ramifications, because the new Internet platform isn't employed in enough real-world situations.

A 2006 report by the U.S. Government Accountability Office (GAO) found that federal agencies have taken some steps in planning for IPv6 conversion, but several agencies have not yet completed important parts of the process. Many Asian nations, particularly China and Japan, have been far more aggressive in pushing along implementation of IPv6.

Ten of the 24 major agencies surveyed by the GAO still had not developed IPv6-related policies and enforcement mechanisms at the time the report was being prepared. The report's authors found that many agencies were not ready to capitalize on the advantages of IPv6, largely because they lacked incentives to use IPv6 or because they weren't far enough along in the transition process. And although 23 of the 24 agencies had at least begun an impact analysis of IPv6, only nine had assessed the costs associated with IPv6 conversion.

The federal government has set clear and laudable goals for IPv6 implementation, but so far actual conversion from IPv4 to IPv6 has fallen far short of those goals. Experts may speculate about IPv6, but its actual data security and privacy strengths and weaknesses won't be fully known until after the new platform is in widespread, day-to-day use throughout the world.

How Does IPv6 Affect the User Privacy and Data Protection Landscape?

The uncertainties of IPv6 create security concerns for both companies and individuals. The ability to collect and transmit massive amounts of data instantaneously is a blessing and a curse: Although this capacity has revolutionized how business is transacted, it also has put confidential customer and employee information at risk as it has never been before. The broader the access, the greater the risk, and IPv6 carries with it no small amount of concerns in that regard.

With its potential for stateless autoconfiguration of unique IP addresses, IPv6 can expose users to greater privacy risks. This autoconfiguration technology opens up the potential to track the same unique identifying number embedded in an IPv6 address each time a user obtains or exchanges information over the Internet. The first 64 bits of an IPv6 address describe the network and can change across connections to different networks. The second 64 bits of the IP address make up the "interface identifier," which stays the same in autoconfiguration for a particular device or host. Some have called this globally unique interface identifier "a second Social Security number."

The total of consumers' IPv4 addresses, in contrast, is only 32 bits. Often, these addresses do not have an embedded number that is constant and unique, because IPv4 technologies frequently change the IP addresses assigned to a particular computer. Organizations that collect the IP addresses of consumers may need to review their privacy notices regarding the collection of a globally constant and unique number in IP addresses of IPv6 users. If an IPv6 laptop computer is autoconfigured with a globally constant interface identifier in the IP address, geo-privacy issues arise when that computer is used in different locations—on a business trip, for example. The same interface identifier in the address can be tracked every time the traveler uses his or her laptop computer in different locations. There are some optional fixes for the IPv6 autoconfiguration privacy issues; instead of using a unique, unchanging identifying number, for example, each user can receive a periodically changing pseudo-random number.

The improved Internet platform also can be used to provide better protection for online users. The European Commission's IPv6 Task Force for the International Working Group on Data Protection in Telecommunications calls IPv6 a "potentially powerful tool to improve the possibilities of user privacy." Built-in security and privacy features of IPv6 provide protections for users that do not exist in most implementations of the current Internet Protocol. However, to be truly effective, those features must be supplemented by the user's own data security efforts.

Another security challenge is political, not technical. Governments and law enforcement agencies continue to push for greater access to personal information as part of the global war on terror. As IPv6 expands the Internet into new areas of communication, it stands to reason that law enforcement may seek greater oversight with respect to these areas as well. One commentator has recommended transition in public and private networks to IPv6 to improve tracking and tracing of IP communications for counterterrorism purposes. Law enforcement agencies will still need to grapple with the fact that IPv6 supports an optional "privacy extension" that can be used to change the interface identifier with every different connection to the Internet, making it more difficult for law enforcement to trace Internet activity to a particular computer or person.

Measures To Improve Online Security in IPv6

One major positive step is that Internet Protocol security (IPSec) is mandatory with IPv6, whereas it is only optional in IPv4. IPSec is a set of protocols designed to make sure that information "packets" are securely exchanged between computers at the IP level. The system provides the user with some protection against data theft, hacker attacks, and theft of users' credentials.

No single entity has full control of IPv6 implementation, but many of the major parties involved at least realize that privacy and data protection are real and urgent considerations. In 2002, the European Commission stated, "Due to the fact that the Internet has, from the very beginning, been considered as an open network, there are many characteristics of its communication protocols, which, more by accident than design, can lead to an invasion of privacy of the Internet users. … It is therefore indispensable that the European Commission and the European Union as a whole consider privacy issues in the further development of the Internet."

The International Working Group on Data Protection in Telecommunications published a 10-point overview plan back in 1996, and its recommendations remain valid today. The group's recommendations have not and probably will not be adopted on any type of worldwide basis, but they represent a consensus of IPv6 experts and, as such, their recommendations should carry a great deal of weight during IPv6 implementation. The Working Group's 10 points are as follows:

1. Service providers should inform each potential user of the Internet unequivocally about the risks to his privacy. She will then have to balance these risks against the expected benefits.
2. In many instances the decision to enter the Internet and how to use it is subject to legal conditions under national data protection law.
3. Initiatives to arrive at closer international cooperation, even an international convention governing data protection in the context of trans-border networks and services, are to be supported.
4. An international oversight mechanism should be established which could build on the existing structures such as the Internet Society and other bodies. Responsibility for privacy protection will have to be institutionalized to a certain extent.
5. National and international law should state unequivocally that the process of communicating (e.g., via electronic mail) is also protected by the secrecy of telecommunications and correspondence.
6. Furthermore, it is necessary to develop technical means to improve the user's privacy on the Internet. It is mandatory to develop design principles for information and communications technology and multimedia hard[ware] and software, which will enable the individual user to control and give him feedback with regard to his personal data. In general, users should have the opportunity to access the Internet without having to reveal their identity where personal data are not needed to provide a certain service.
7. Technical means should also be used for the purpose of protecting confidentiality. The use of secure encryption methods must become and remain a legitimate option for any user of the Internet. The Working Group supports new developments of the Internet Protocol (IPv6), which offer means to improve confidentiality by encryption, classification of messages and better authentication procedures. The software manufacturers should implement the new Internet Protocol security standard in their products, and providers should support the use of these products as quickly as possible.
8. The Working Group would endorse a study of the feasibility to set up a new procedure of certification using "quality stamps" for providers and products as to their privacy-friendliness. This could lead to an improved transparency for users of the Information Superhighway.
9. Anonymity is an essential additional asset for privacy protection on the Internet. Restrictions on the principle of anonymity should be strictly limited to what is necessary in a democratic society without questioning the principle as such.
10. Finally, it will be decisive to find out how self-regulation by way of an expanded "Netiquette" and privacy-friendly technology might improve the implementation of national and international regulations on privacy protection. It will not suffice to rely on any one of these courses of action: they will have to be combined effectively to arrive at a Global Information Infrastructure that respects the human rights to privacy and to unobserved communications.

You may say: That's all fine, but what should *my* organization be doing to address IPv6 privacy and security issues? Here is a starter list:

1. Understand the new technology capabilities of IPv6 and make a business decision about whether, when, and how your organization will implement IPv6 or become IPv6-ready. The European Union is aggressively supporting IPv6 to achieve a global competitive advantage.
2. Understand the security-enhancing features of IPv6 as well as the features of IPv6 that raise new challenges to the security of data. Design and build IPv6 security in your network from the beginning; you have a fresh start (as opposed to the current environment of 20 years of IPv4 security patches and add-ons).
3. Understand and address the security challenges in transitioning from IPv4 to IPv6. Even if you move your entire organization to IPv6, your trading partners and the rest of the world will not all move to IPv6 at the same time that your organization does. IPv6 clients (for example, personal computers) in your organization will still need to communicate with the outside world.
4. Understand and address the security threats to your organization's IPv4 network devices (such as firewalls, routers, and the like) and clients from incoming IPv6 traffic that exists today. Even if you decide that you do not need to transition your systems to IPv6 in the foreseeable future, hackers are already using IPv6 technologies to attack IPv4 systems. For example, unless a system administrator implements proper protective controls, an attacker may be able to send IPv6 malicious code through an IPv4 "tunnel" and install backdoor programs on an IPv4 host or client that do not show up in IPv4 security scans. Also, IPv4 firewalls

may need to be specifically configured to recognize and filter IPv6 traffic.

5. Make sure you identify IPv6 clients who may be accessing your network without your knowledge. For example, an employee may connect a personal computer with Windows Vista™ software to your network. Because Windows Vista is shipped with IPv6 "default on," through IPv6, the program could be revealing its site-local address within your network to outsiders, thus exposing the computer to new threats by attackers. Also, users can easily self-install IPv6 in computers that have Windows XP™ software installed, and in some network configurations the network administrator will not be able to detect the IPv6 installation.
6. Incorporate IPv6 security risk management into your supply chain processes. Do this for technology acquisitions and also to protect against vendors and business partners who have access to the organization's sensitive information, including trade secrets and sensitive personally identifiable information. Just as your own organization needs to manage IPv6 security challenges in its own systems, your organization should address how its vendors are addressing IPv6 in their systems.
7. IPv6 calls for a fundamental re-evaluation of basic information security models. In IPv4 networks, the "perimeter defense" concept prevails; this means there are protective firewalls, gateway routers, internal routers, and other devices that stand between the Internet and the network's hosts and clients (personal computers, for example). In contrast, the "plug-n-play" nature of some IPv6 implementations can mean that there is a virtual network that is distributed beyond an organization's "perimeter." There is no perimeter firewall; distributed devices have their own individual firewalls. According to Tom Patterson, chief executive officer of Command Information, an IPv6 consulting and testing company, "In short, if you proactively address IPv6 security, you can get more security for a lot less money. Conversely, if you ignore the security changes that come with IPv6, you'll end up with a lot less security for a lot more money."

Conclusion

Internet Protocol Version 6, should not be considered a magic bullet that ensures user privacy any more than it should be looked upon as a step backward for data protection. Instead, IPv6, like the current Internet Protocol, provides both opportunities and challenges for information privacy and protection. The onus ultimately will remain on administrators and users of IPv6 technology to ensure that data related to their employees, customers, and clients are stored and transmitted securely.

Michael W. Hubbard is the leader of Womble Carlyle's Privacy and Data Protection Team and practices in the firm's office in Raleigh, N.C.

References

(All sites last visited on Aug. 9, 2007)

Comments before the National Institute of Standards and Technology (March 8, 2004), www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/comments/EPIC_IPv6.htm.

Communication from the Commission to the Council and the European Parliament, *Next Generation Internet Priorities for Action in Migrating to the New Internet Protocol IPv6* (2002), eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52002DC0096:EN:HTML.

Convery, Sean, and Darrin Miller. *IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v 1.0)* (2004), www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf.

Davies, Joseph. *IPv6 Improvements in Windows Vista*, 6SENSE NEWSLETTER (2006), www.usipv6.com/6sense/2006/apr/01.htm.

International Working Group on Data Protection in Telecommunications. *Draft Report and Guidance on Data Protection on the Internet* (May 1996), trout.cpsr.org/cpsr/lists/rre/Data_Protection_and_Privacy_on.

Kaisor, Basar, et al. *IPv6: Legal Aspects of the New Internet Protocol* (Euro6IX, 2005), www.ipv6tf.org/pdf/ipv6legalaspects.pdf.

Marsan, Carolyn Duffy. *Windows Vista Not Playing Well with IPv6*, PCWORLD (2007), www.pcworld.com/article/id,132689-c,vistalonghorn/article.html.

National Telecommunications and Information Administration. *Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)* (January 2006), www.ntia.doc.gov/ntiahome/ntiageneral/ipv6/final/ipv6final.pdf.

U.S. Government Accountability Office. *Internet Protocol Version 6: Federal Government in Early Stages of Transition and Key Challenges Remain* (June 2006), www.gao.gov/new.items/d06675.pdf.

Warfield, Michael H. *Security Implications of IPv6*, INTERNET SECURITY SYSTEMS 2003, documents.iss.net/whitepapers/IPv6.pdf.

Westby, Jody R. *Countering Terrorism with Cyber Security* at 14 (August 2006), www.cyberconflict.org/pdf/JodyWestby-WFS-TerrorismFlourishesPaperv6.pdf.