Questioning IPv6 Security

Laura DeNardis, Ph.D.

IPv6 requires IPSec, so it's more secure than IPv4, right? Wrong and wrong.

One commonly cited rationale for upgrading to IPv6 is the claim that the newer Internet Protocol provides vastly improved security over IPv4. This article describes how conceptions of IPv6 as more secure than IPv4 are somewhat misleading and how implementation realities indicate that IPv6 can actually create a less secure enterprise network environment.

The IPv6 Security Narrative

The IETF selected IPv6 as an incremental protocol upgrade primarily intended to expand the number of unique Internet addresses from roughly 4.3 billion to 3.4 x 10^{38}. Assertions that IPv6 also improves security have emanated from the U.S. Department of Defense, media outlets, network industry publications, IPv6 advocacy groups and international entities upgrading to IPv6. This security claim often exists as a common denominator under diverse expectations for the protocol, ranging from promoting Third World development to improving U.S. military capability.

Beginning in 2000, Asian and European Union governments developed national IPv6 upgrade strategies, citing the enhanced security features of IPv6 as one benefit for upgrading, in addition to the expanded IP address space and what they considered the possibility of becoming more competitive in Internet markets by developing IPv6 products and expertise.

In 2003, the U.S. government published the National Strategy to Secure Cyberspace, the culmination of a lengthy analysis seeking to reduce vulnerability to cyberterrorism and critical infrastructure attacks. One of the Strategy's recommendations called for improvements in the security of several network protocols, including IP. The Strategy noted that Japan, the European Union and China were already upgrading from IPv4 to IPv6 and cited improved security as one of the benefits of IPv6. Though IPv6 received only this cursory mention, the U.S. Strategy asserted as an unquestioned fact that IPv6 improved Internet security.

In the same time frame, the U.S. Department of Defense announced that it would transition to IPv6 by 2008, citing the requirement for end-to-end security, as well as more addresses for military combat applications. Testimonies in the 2005 congressional hearings on IPv6 before the House of Representatives Committee on Governmental Reform similarly claimed that IPv6 provided improved security.

Not surprisingly, advocacy groups promoting worldwide IPv6 deployment laud IPv6 security features, along with other justifications, as a rationale for upgrading, and technology vendors with a stake in IPv6 adoption cite enhanced security as well. The notion that IPv6 improves Internet security is obviously widespread and presented as a self-evident truth.

Conflating IPSec And IPv6

One of the reasons for this linkage between IPv6 and security is the historical association between IPv6 and a separate network layer protocol, IPSec.

The early Internet and its predecessor networks involved relatively closed information exchange among trusted individuals who shared a strong educational and professional familiarity. But as the Internet transformed into a more expansive and global network, and after network security vulnerabilities and disruptions occurred, security became more of a concern to Internet technical designers, and was retrofitted into network protocols.

Correspondingly, security was a design consideration during the 1990s' development of the IPv6 standard, and drove the initial IETF-mandated inclusion of IPSec (through Authentication and Encapsulating Security Payload extension headers) within the early IPv6 draft specifications. IP does not intrinsically provide security, but this theoretical linkage between the early IPv6 protocol specification and IPSec forms one origin for the claim that IPv6 improves security.

However, several circumstances suggest that IPv6 is not necessarily more secure just because of the "mandated" inclusion of IPSec in the IPv6 specification.

First, IPSec encryption can be—and often is—implemented in IPv4 networks as well as in IPv6 networks. The argument that IPSec improves the security of IPv6 networks is equivalent to the argument that IPSec improves the security of IPv4

Laura DeNardis is a computer networking and security analyst residing in Stamford, CT, and a 2006–2007 Visiting Fellow at the Information Society Project (ISP) at Yale University. She holds engineering degrees from Dartmouth (A.B.) and Cornell University (M.Eng.) and a Ph.D. in Science and Technology Studies from Virginia Tech.

networks. It is the encryption provided by IPSec that provides security, not the IPv4 protocol or the IPv6 protocol. In network implementations, IPSec provides no more or less security in conjunction with IPv6 or with IPv4.

Second, while IPSec was a required element in earlier IPv6 specs, later IPv6 revisions dropped IPSec as a *requirement*. Specifically, the IETF's 1995 IPv6 draft standard (RFC 1883) required IPSec encryption with IPv6, but the specification was updated in 1998, at which time the *compulsory* dependency between the IPv6 specification and IPSec was eliminated. The bottom line is that, in practice, many IPv6 implementations do not implement IPSec.

Finally, even if the use of IPSec within the IPv6 specification made IPv6 networks more secure than IPv4, it's important to acknowledge that the encryption provided by IPSec—itself not necessarily the preferred form of network encryption—is only one part of a network security framework most corporations or institutions require. Encryption protects the privacy of information as it traverses a network and can address data integrity and user authentication. IPSec does not protect against viruses, worms and spyware, nor battle distributed denial of service attacks, to name a few security issues. IPv6, like IPv4 and IPSec, operates at the network level, not the application level where some security attacks occur. Although the immense IPv6 address space significantly retards attacks based on network scanning for addresses (ping sweeps), ultimately IPv4, IPv6, and IPSec are significantly removed from application-level security attacks.

IPSec is, in fact, not a v6 requirement

In summary, then, the conflation of IPv6 and IPSec is behind some of the claims of IPv6's enhanced security, but this picture is misleading because it assumes:

1.) That IPv6 implementations, in practice, always use encryption.

2.) That IPv4 networks cannot use IPSec encryption; and/or

3.) That encryption such as provided by IPSec provides even close to a comprehensive security framework.

IPv6 Security Vulnerabilities

Rather than providing "improved security" or specifically addressing security at all, IPv6, a less mature protocol than IPv4, actually raises some security issues users must address. For example, most network devices and operating systems incorporate features allowing users to configure networks for IPv6 traffic or applications. Even for users exclusively employing IPv4, this IPv6 capability is still present and still raises security considerations.

As with most developing protocols, security weaknesses have been identified in IPv6-enabled products, and these require user action to mitigate. Users not specifically employing IPv6 capabilities might assume the security vulnerabilities and associated patches are inapplicable to their network environments and forego the necessary network security responses.

We've seen this in the U.S., where federal government agencies, rather than large corporations, have taken the lead in IPv6 adoption. Even in the context of federal IPv6 momentum, U.S. government studies have recognized that IPv6 can present security challenges, rather than improving security. For example, a 2005 Government Accountability Office (GAO) analysis of IPv6 identified security risks as a significant transition consideration for federal agencies.

The U.S. House of Representatives Committee on Government Reform requested that the GAO perform an analysis auditing the progress the DoD and any other government agencies have made in transitioning to IPv6 and identifying considerations for agencies upgrading or planning to upgrade. The GAO's findings, in a report entitled "Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks" (GAO-05-471: May, 2005), stressed that dormant IPv6 capability actually *exacerbated* security risks rather than mitigating risks. For example, an employee enabling IPv6 capability might create an inadvertent security problem because an institution's security system configuration might not detect breaches exploiting IPv6 features.

The GAO audit specifically investigated two IPv6 characteristics, automatic configuration and tunneling, for security vulnerabilities. The audit confirmed widely understood security vulnerabilities of these features and determined that they posed serious potential risks to federal agencies.

Protocol designers included automatic configuration as an IPv6 feature intended to simplify network administration of IP addresses. This autoconfiguration feature might permit an unauthorized router connected to a network to derive an IPv6 address from neighboring routers without manual configuration. In other words, an unauthorized user could connect to a network without local authorization or registration.

Similar security vulnerabilities are associated with tunneling, the technique of transmitting IPv6 packets over an IPv4 network. The embedding of IPv6-formatted information within IPv4 packets can allow potentially unauthorized activity to occur undetected by firewalls.

Consistent with the evolution of most protocols, a number of intrinsic security vulnerabilities have been identified in IPv6 systems. The history of IPv6 deployment includes the ongoing history of the identification of IPv6 security vulnerabilities and development of associated solutions.

Mixed v4/v6 deployments will further complicate security

Cisco has issued advisories about vulnerabilities in products running Cisco IOS which are IPv6 enabled. (Cisco Security Advisory Document ID: 65783) As Cisco has indicated, without recommended patches, devices running IOS are susceptible to denial of service attacks and arbitrary code attacks. Juniper customers using M-Series and T-Series IPv6-enabled routing platforms similarly received notification to upgrade software to correct a vulnerability potentially enabling denial of service attacks (US-CERT Vulnerability Note VU#658859). Protocol vulnerabilities susceptible to denial of service attacks were also found in HP Jetdirect IPv6/IPSec Print Servers (US-CERT Vulnerability Note VU#226364) and in Sun Solaris 8 systems accepting IPv6 traffic. (US-CERT Vulnerability Note VU#370060).

IPv6 is a less mature protocol than the long-prevailing IPv4, so the ongoing identification of protocol-specific product vulnerabilities is not unusual. Each vulnerability pronouncement necessitates user action such as the installation of vendor-issued software patches and upgrades. Again, users not cognizant of IPv6 features inherent in products might assume IPv6 security advisories to be inapplicable, leaving vulnerabilities unaddressed.

Mixed IPv4/v6 Implications

Those claiming IPv6 is more secure than IPv4 usually operate under the assumption that a network would be entirely IPv6 end-to-end. One justification for describing IPv6 as more secure, resting on this end-to-end IPv6 assumption, is the elimination of Network Address Translation (NAT).

NAT devices conserve IP addresses by allowing numerous devices to share public IP addresses. NAT devices employ limited public IP addresses to mediate, presumably in response to IPv4 address constraints, between a private network with many private IP addresses and the public Internet.

This type of device is a network intermediary disrupting the end-to-end flow of information across the Internet and therefore constraining the application of end-to-end security mechanisms like encryption. But this end-to-end security vision would be somewhat of a chimera even if NAT boxes were completely eliminated.

First, other network intermediaries, especially firewalls and intrusion detection systems, would continue (and should continue) to be deployed. Network intermediaries will continue to exist in enterprise networks, and some IPv4/v6 transition strategies themselves can rely on translation techniques.

Second, it may be argued that NAT actually can improve security as an intermediary masking external network visibility into a network's internal IP addresses.

Additionally, implementation realities, especially in the U.S., indicate that IPv4 and IPv6 will coexist for the foreseeable future, negating the possibility of security benefits from IPv6-only environments; such environments simply will not exist in very many places.

There are several approaches to transitioning from IPv4 to IPv6, or for supporting the ongoing use of both protocols: dual stack, tunneling, and translation. The dual stack option involves installing separate suites of IPv4 and IPv6 software on routers and hosts. Applications employ either IPv4 or IPv6 based on IP address or a preprogrammed preference.

An alternative technique, tunneling, encapsulates packets of IPv6 information within IPv4 packets for transmission over an IPv4 network or, inversely, encapsulates IPv4 packets within IPv6 packets before traversing an IPv6 network.

The third approach, translation, enables devices only supporting IPv4 to communicate with devices only supporting IPv6 by translating IPv4 packets entirely into IPv6 packets or vice versa.

Each approach presents a different set of challenges, requires administrative and processing resources, and affects network security frameworks. Rather than simplifying security, mixed protocol environments can actually complicate security (as well as network management). For example, tunneling one protocol through another network protocol can enable unauthorized traffic to traverse a network, including passing through a firewall undetected. When using the dual-stack approach, attacks can target both IPv4 and IPv6 applications, and security measures must be applied to both protocol versions.

Bottom Line

Considering implementation realities, IPv6 is not the security panacea many entities claim it to be. There are many reasons for considering IPv6, depending on network requirements and existing IP address resources, but improved security is really not one of them.

Implementation realities suggest IPv4 and IPv6 will coexist for the foreseeable future, potentially complicating security and management. IPSec, while itself not at all a comprehensive security solution, can operate equally well in IPv4 and IPv6 networks.

IPv6, like most evolving protocols, has experienced its share of intrinsic security vulnerabilities. Claims that IPv6 improves security are misleading and run the risk of promoting complacency about the specific security measures and broad frameworks required in most enterprise network environments with either dormant or enabled IPv6 capabilities□