IPsec in IPv6 - The Plain Truth

Coming next - a comparison of Internet Protocol (IP) security (IPsec) protocol that provides interoperable, cryptographically-based security services that authenticate and/or encrypt each IP packet of a data stream. What are the advantages of IPv6 - based IPsec built into IPv6 stacks? Is IPsec a “killer app” for IPv6 that will revolutionize security? What are the real advantages to IPv6 vs. IPv4 IPsec?

IPSec for both IPv4 and IPv6 is deployed at layer-3 (networking layer) to provide security to protect *all* Internet-capable applications. Competing Internet encryption/authentication systems in widespread use today, such as Secure Sockets Layer (SSL), Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers of the TCP/IP model, only protect specific types of applications, and are generally more vulnerable to man-in-the middle attacks.

IPsec features and their functions for both IPv4 and IPv6 are:

- Authentication Header (AH) provides connectionless integrity (data has not been modified) and data origin authentication (sender authentication and non-repudiation proof that sender, not a 3rd party, did send the message) for IP datagrams and to provide protection against replay attacks.
- Encapsulating Security Payload (ESP) to provide confidentiality (data encryption) and/or integrity-protection, data origin authentication, access control (used for VPN tunneling into networks) , replay protection (partial sequence integrity), and limited traffic analysis protection
- Internet Key Exchange (IKE and the newer IKEv2) protocols allows peer devices to negotiate which IPsec protections will be applied, which types of traffic will receive the protection (traffic selectors), and what cryptographic algorithms will be used. These specifics, along with the identities of the communicating peers, comprise a Security Association (SA). IKE also negotiates, manages, updates and deletes the secret keys used by IPsec.

IPsec encryption can be deployed in standalone environments between host clients, routers, and VPN gateways in the following three scenarios

- Host to Host – This protects communications directly between peers such as PCs or routers. This feature greatly enhances the security against on-link insider threats on networks, but is not commonly deployed today for reasons which will be discussed in the section on deployment.
- Host to Gateway – This is the common deployed Virtual Private Network (VPN) scenario used to give hosts remote access to a private enterprise network through an encrypted tunnel between the host and a VPN gateway
- Gateway to Gateway – This is commonly used for bulk encryption VPN gateways or as encrypted tunnels between routers between enterprise subnets or to give remote enclaves access to a private secure network. An example is the US DoD High Assurance IP Encryptor (HAIPE) which is used to connect remote enclaves into the Global Information Grid (GIG).

IPsec State of Deployment: The host to gateway and gateway to gateway IPv4 IPsec models are well deployed today in our system of VPNs and site-to-site bulk encryption gateways, so we will examine

the deployment limitations of the newer host-to-host model often touted as a “killer applications” for IPv6. Many security experts envision that layer-3 IPsec deployed in IPv6 (and IPv4) stacks will supplement gateway to gateway bulk encryption and host to gateway VPNs with an additional capability allowing communicating peers to directly protect their traffic. This host-to-host IPsec scenario can enhance security against on-link insider threats which are not well addressed in the host-to-gateway or gateway-to-gateway model. It is relatively easy to deploy small manually configured enclaves of peers supporting the host-to-host IPSec model, but before the vision of large-scale deployments can be realized, we will have to create and deploy tools and support infrastructure to scale IPsec deployment. In order for IPsec to scale to a practical system, it must be coupled with a Public Key Encryption (PKI) system and an automated Internet Key Exchange (IKE and IKEv2) protocol so the peers can automatically establish each others’ definitive identities, determine each other’s access levels, and exchange session keys for a security association. To create and automated system to scale IPsec beyond a small enclave, an organization needs a PKI and a secure user database, such as the US DoD Common Access Card (CAC) system & Microsoft Active Directory, to support authorization and key exchanges between IPsec peers. Another deployment concern is that IKE and IKEv2 which automate the exchange of session keys for IPsec are recently standardized protocols and are not yet widely deployed. A third concern limiting the deployment of direct host-to-host IPsec model we have no good way to monitor and authorize the encrypted host-to-host sessions with our current security tools. Once PKI systems and security tools are upgraded to better support the host-to-host IPsec scenario, this technology can be deployed to upgrade our networks for a better defense in depth - especially against compromised on-link threats.

IPsec for IPv6 Advantages: The implementations for layer-3 IPsec are almost identical for IPv4 and IPv6. Data analyzed from the VPN Consortium survey of IPsec implementation http://www.vpnc.org/vpnc-ipsec-features-chart.html and from our experience with multiple IPv6 IPsec products leads us to the conclusion that all major IPsec implementations for IPv6 have IPv4 implementations available too. One possible advantage for IPv6 IPsec is that IPv6’s extension header chaining feature, which is not present in IPv4, could be used to authenticate a secure host-to-host scenario exchange to a third party gateways which would provide authorized access into and out of secure enclaves. The common use of private IP addressing and Network Address Translation (NAT) in many IPv4 networks also complicates the deployment of the direct host-to-host IPsec as the translation of IP headers at NAT gateways interferes with IPsec authentication. The problem of NAT interfering with host-to-host IPsec exchanges does not apply when IPv6 is deployed with its native end-to-end addressing and connection model. IPv6 NAT traversal tunneling “transition mechanisms”, designed to make it easier to deploy IPv6 through IPv4 NAT, also make it easier to deploy IPsec through NAT.

IPSec for IPv6 Conclusions: IPsec as implemented in the IPv6 and IPv4 stack of most operating systems COULD provide an enhanced security service for host-to-host (aka peer-to-peer and/or machine-to-machine) communications once we mature the management tools and support infrastructure required to move beyond manual configurations and implement it on a larger scale. IPv6 offers some improvements to IPv4 IPsec implementation, but the enhancements are hard to capitalize on in the short term. IPv6 main advantages may be its ability to provide an enhanced end-to-end connection model for host-to-host IPSec and its ability to scale to support Internet-based communications (and IPsec) beyond the next decade when IPv4 scaling reaches its limits.

This entry was posted on Sunday, March 15th, 2009 at 10:47 pm and is filed under Blog: Information Assurance, Federal Enterprise Architecture, Blog: IPv6. You can follow any responses to this entry through the RSS 2.0 feed. You can leave a response, or trackback from your own site.