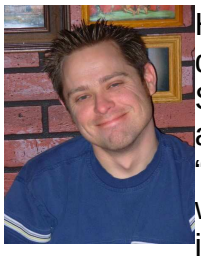
I feel like I've been lied to..



Hyperbole aside, it seems like IPv6 over-promised what it was never intended on delivering. So I feel like I have been lied to. I can remember my first IPv6 Summit/Conference, and there was always one item that struck me as fascinating and amazing: IPv6 is more secure because it ***mandates*** use of IPSec. I remember thinking, "Wow, every node on the network must use end-to-end authentication and encryption with IPv6!" Only months later in researching IETF, my optimism would be crushed. So if I just crushed your childhood fantasy of IPv6, please let me explain.

The birthing of IPv6 and IPSec..

Back in 1995, RFC 1883 was written. This was the original IPv6 standard. Maybe this is where the myth emerged? Take a look at Section 4, it states "A full implementation of IPv6 includes implementation of the following extension headers … Authentication (AH) and Encapsulation Security Payload (ESP) Read more: http://www.faqs.org/rfcs/rfc1883.html#ixzz0czwMCI2P. So many standards since this have either reiterated it or strengthened this statement. RFC 4295 (IPv6 Node Requirements, April 2006) states that all nodes in a network must support the basic security architecture including ESP and AH. This includes routers, workstations, simple network appliances, etc must support IPSec AH and ESP. This is great right? Except we have two very real problems.

Then what's the reality?

Problem # 1: Equipment manufacturers began inserting an entirely new networking stack in order to include basic support for IPv6. Since IPv4 and IPv6 are not backwards compatible (and supporting IPv6 is not a light switch) the device still needs to support basic IPv4. So many of these vendors had to make a prioritized feature list. Well, IPSec lost. Only on a few select network appliances you find full IPSec support over IPv6. They weren't ignorant in this decision, because networks are not using IPSec on a host-to-host level. Most enterprise networks use IPSec for site-to-site VPNs, or host-to-VPN connectivity. Rarely is it used for a host to authenticate and encrypt communications over IPSec to print a document, connect to a mail server, or pull down a web page. In fact the very idea of it seems like a very different security architecture.

Basically, the vendors called it. They didn't do this in a vacuum because networks just don't use these functions today. So why can't the user community just force these vendors to support it? The use case seems out of grasp for most enterprise networks. This brings us to problem number 2.

Problem #2: The overall security paradigm must ***completely change***. I encourage you to take a tour of your network facility, and see just how many perimeter security devices there are; then take a look at the hosts in the network. These hosts will likely only have simple anti-virus software. Most networks will have a multi-layer perimeter security architecture comprised of firewalls, intrusion detection and prevention systems. These systems trust nothing. So even if an IPv6 node would want communicate outside of the enterprise, it would not be allowed. The reasons centers on only one thing: trust. Network security is only done at the perimeter. There are a few host-based security systems out there, but these are not the primary means to secure the network. Cybersecurity has become such an issue that this architecture is already being pulled apart. As hosts communicate more over SSL (HTTPS), the perimeter security must trust or disallow these communications as well.

Is there a secure way?

Absolutely, integrating IP Security and application security. The DoD uses a system called Public Key Infrastructure (PKI) that can easily be configured to manage keys at layer 3 instead of layers 6 and 7. Each node on DoD networks are being required to support a smart card PKI system. Currently, it's built to establish an SSL authenticated session. However, it is one more step to manage public keys for IPSec keys using systems like Internet Key Exchange Version 2 (IKEv2) and associated encryption algorithms. So long as the system is configured properly combined with a robust host-based intrustion security system, security professionals would be more apt to allow end-to-end IPSec. However, if these two systems are not available, then will IPSec will never be allowed with IPv6.

So do you feel lied to as well? Or do you have something to say about this as well? Let me hear you in the comments below!

This entry was posted on Monday, January 18th, 2010 at 5:21 pm and is filed under Jeremy Duncan, Cybersecurity, Blog: IPv6.