



COA¹ Position Paper Encapsulation & Encryption

Problem

How you make a secure, trusted connection over the Internet is one of the key debates as the industry strives for de-perimeterised solutions that it can implement.

To the charge that the protocols they are using are inherently insecure; the un-enlightened reply from the industry is “no problem we can encapsulate it in a VPN tunnel”, to which usually they mean an IPSec tunnel.

Response

The use of VPN tunnels, while appropriate in a few cases to solve particular security problems (see later), has no place in a de-perimeterised future.

A laptop on the end of an IPSec tunnel may have been authenticated onto the network with two-factor authentication, even end-point checked, but is still as vulnerable to the worm, virus or hacker, the same as any other computer on the network to which the IPSec tunnel terminates.

Background & Rationale

Tunnels are Point to Point

A tunnel is just that; it connects a start to a destination and forces all traffic to go down it. In the corporate environment, that IPSec tunnel is often used to connect remote computers into the corporate environment, by extending the corporate perimeter to the device in question.

Even though the resources you are trying to access may be a few miles away, your data may travel half way round the world to where the tunnel terminates only to return to the system you are trying to access.

Tunnels are generally singular

Most VPN tunnels are set-up as singular entities, there is no concept of the opportunistic creation of on-the-fly tunnels or the creation of multiple tunnels each with the most efficient route for each transaction.

In a de-perimeterised world a device should be routed to its resources by the most efficient method. Moreover, individual application on a device should each be able to be individually routed to their destination.

¹ Collaboration Oriented Architectures (COA) paper and COA Framework paper, both available from the Jericho Forum publications page at <http://www.opengroup.org/jericho/publications.htm>

Tunnels need creating

The creation of an encapsulated, encrypted tunnel requires negotiation and setup, not only for authentication but also negotiation of the standards to be used. Generally trying to get a reliable tunnel created between two different vendors usually impossible, and certainly not reliable for ad-hoc or on-the-fly tunnel creation.

Inspection, or lack of it

Whereas an inherently secure protocol using either IPv4 or IPv6 will allow limited inspection, even if the data cannot be read, data encapsulated in a tunnel cannot be inspected in any way, all that can be understood is the start and termination points of the tunnel.

There are circumstances where this may be desirable, where the anonymity of the packets is desirable because of deduction that could be made from the headers, however if security at this level is required, IPSec will almost certainly not be the technology of choice.

Where to use

VPN tunnels are a valid stop-gap solution for connecting remote workers back into the still-perimeterised corporate environment.

Site-to-site connections or island-to-island connections, where an area of secure connectivity is connected to another area of secure connectivity. In the transition to a de-perimeterised architecture this will be a useful tool.

System to system; here a system that requires to be semi-permanently connected to another system could validly use a VPN tunnel

Where not to use

Tunnelling technology should not be used to encapsulate a single protocol. For example to extend VoIP from a corporate environment to a home worker.

Neither should it be used to encapsulate insecure protocols where secure protocols are available; for example FTP and sFTP,

SSL VPN's

While a different technology, as their proponents try to mirror the features and advantages of IPSec VPNs so the same issues arise.

Challenges to the industry

1. Companies should plan for remote working solutions that do not rely on VPN tunnels but instead utilise inherently secure solutions, allowing working directly in the Internet.
2. The industry should reject the use of VPN's to encapsulate insecure protocols, and work to support, use and develop inherently secure alternatives.

The way forward

The Jericho Forum believes that encapsulation via IPSec, while a valid current stop-gap solution, has little place in a de-perimeterised future for Internet security and should not continue to be used as an excuse to not fix the current insecure protocols at their root cause.
