

Is SMTP too simple?

Kevin Green

THE RISING TIDE of unsolicited e-mail and malicious viruses threatens to choke the Internet despite the best efforts of vendors and users to stem the tide of cyber junk.

Gartner estimates that spam now accounts for more than 50 percent of all e-mail sent, with some sources putting the figure as high as 60 to 70 percent.

German antispam group Spamhaus.org, has identified five of the top 200 spammers as being Australian.

The talk in chat rooms and among industry observers is that neither filtering technologies or regulation will stem the tide and that alterations to the 20-year-old e-mail standards protocol should be considered.

The protocol that facilitates e-mail, Simple Mail Transfer Protocol (SMTP) was adopted in 1982 when e-mail use was largely an academic pursuit of community-minded individuals.

Exponential growth in e-mail during the 1990s in line with the rapid growth in Web usage has led to calls for changes to be made as e-mail management costs spiral.

SMTP lets senders mask both their identities and servers, thus spammers using randomly generated addresses crank out e-mail in relative anonymity.

The use of open architecture of the old POP3 or Internet Message Access Protocol facilitates their efforts.

Therefore authentication and identity of senders is acknowledged as being the key issue to be resolved.

The US-based Internet Engineering Task Force (IETF) is taking submissions from interested bodies globally to look at SMTP via its AntiSpam Research Group (ASRG). Among the proposals the ASRG is studying is one to change the domain name system so that legitimate IP addresses can be associated with authenticated domains.

A fundamental question to be addressed is, should SMTP be rewritten, changed or have another layer added to it?

Cynics comment that the IETF's ratification of any new protocol would be long term and cite the slow progress of IPv6, the next version of the Internet protocol, as an example of the pace of change.

Ironport, a global player with a presence in Australia, has made a number of suggestions.

"The key is that SMTP was not created to do what it does today", Michael Bosch, MD of Ironport Systems Australia and New Zealand, said.

Their SMTPi submission to the IETF proposes tackling the main weakness of SMTP — identity — in a way similar to the Domain Name System (DNS) operation.

"Senderbase.org is a publicly accessible database that lists senders of e-mail by IP address and domain name.

"Right now we're processing about 25 percent of the world's e-mail — Microsoft uses it for Hotmail in 110 million mailboxes," Bosch said.

Another approach, taken by European consortium RIPE, acknowledges the difficulty of a global change.

It suggests adding a parallel protocol to SMTP that has tighter authentication, thus allowing both users of the existing SMTP and the new protocol to coexist.

This opt-in approach has merit in that it allows both privacy and legitimacy for those who want it; however, it may still leave a loophole for illicit e-mail use.

Security has always been an issue with e-mail, yet secure e-mail, according to Gartner, accounts for only 2 percent of all e-mail sent.

However, the associated technology of digital certificates is being championed by the ePrivacy Group, a privacy and consultancy vendor, to solve SMTP's lack of authentication.

Eprivacy's approach, TEOS, provides content descriptions and uses existing third-party digital certificates to identify e-mail senders.

There are many sceptics, however, who see global changes and additional complexity as being unrealistic.

"Our view is that you don't know what you are trying to

➤ page 23

Is SMTP simple?

C page 20

do," Leigh Costin, director of product marketing from local vendor Fortinet, said.

"It's like saying we're going to add a third atom to oxygen and I'm not convinced that SMTP has to change.

"SMTP has had remarkably few vulnerabilities apart from the fact that you can send to anyone."

Fortinet, an antivirus company in the telco and SME space, will be releasing its initial filtering product, Fortigate, in June.

Gartner, in its latest research paper, concurs that identification is the issue.

A solution that would extend DNS to DNS Security Extensions (DNSSEC),



COSTIN — I'm not convinced that SMTP has to change

operating like telephone caller ID, is required, the analyst says.

However, Gartner also acknowledges that the industry is crying out for a more immediate fix. "The solutions along the lines of Ironport or more collaborative solutions across industry have the potential for attacking the problem in a more immediate fashion," Gartner analyst Steve Bittinger said.

"It's a very hot market and an incredibly topical boardroom conversation and as a result organizations are investing significant funds into trying to solve problems in these areas." David Taylor, NetIQ regional director of Australia and New Zealand, said.

Meantime, spam, spoofing and the untraceable virus scourge continues in an ever increasing arms race between vendors and spammers with industry paying the bills. ▀