

Re: Current status?

## Re: Current status?

---

*Source:* <http://unix.derkeiler.com/Newsgroups/comp.os.vms/2008-09/msg00506.html>

---

- *From:* [billg999@xxxxxxxxxxx](mailto:billg999@xxxxxxxxxxx) (Bill Gunshannon)
  - *Date:* 11 Sep 2008 12:54:13 GMT
- 

In article <hPXxk.13\$ia.10@xxxxxxxxxxxxxxxxxxxxxxxx>, John Santos <john@xxxxxxx> writes:

Bill Gunshannon wrote:

In article <A4-dnZKGduU09FjVnZ2dnUVZ\_sjinZ2d@xxxxxxxxxxx>, "Richard B. Gilbert" <rgilbert88@xxxxxxxxxxx> writes:

Bill Gunshannon wrote:

In article <zYmdnV7yroyp3VjVnZ2dnUVZ\_v\_inZ2d@xxxxxxxxxxx>, "Richard B. Gilbert" <rgilbert88@xxxxxxxxxxx> writes:

Bill Gunshannon wrote:

In article <KKadnb\_N\_b8StljVnZ2dnUVZ\_vKdnZ2d@xxxxxxxxxxx>, "Richard B. Gilbert" <rgilbert88@xxxxxxxxxxx> writes:

Bill  
Gunshannon  
wrote:

In  
article  
<g9r0lf\$g15\$1@xxxxxxxxxxxxxxxxxxxx>, david20@xxxxxxxxxxxxxxxxxxxx  
writes:

Re: Current status?

Re: Current status?

In  
article  
<7h%vk.609\$393.335@trnddc05>,  
John  
Santos  
<john@xxxxxxx>  
writes:

Bill  
Gunshannon  
wrote:

In  
article  
<g9pl82\$lh7\$4@xxxxxxxxxx  
helbig@xxxxxxxxxxxxxxxxxxxx  
(Phillip  
Helbig---remove  
CLOTHES  
to  
reply)  
writes:

In  
article  
<t\_Wvk.2076\$U5.10  
=?ISO-8859-1?Q?J  
<jan-erik.soderholm  
writes:

Yup.  
I  
think  
that  
many  
of  
the  
problems  
arise  
because  
MUAs  
use

Re: Current status?

Re: Current status?

the  
same  
protocol  
(SMTP)  
and  
port  
(25)  
to  
send  
mail  
to  
MTAs  
as  
MTAs  
use  
to  
relay  
mail  
to  
each  
other.

Modern  
MTAs  
can  
be  
configured  
to  
allow  
mail  
clients  
to  
submit  
mail  
to  
them  
on  
the  
mail  
submission  
port  
(port  
587)  
rather  
than  
port  
25.  
See  
RFC  
2476

Re: Current status?

Re: Current status?

<http://www.faqs.org/rfcs/rfc2476.html>

What  
does  
this  
buy  
you?  
You  
would  
still  
need  
to  
know  
who  
your  
MTA  
is  
and  
it  
would  
still  
need  
to  
be  
willing  
to  
accept  
email  
from  
you.  
It  
is  
all  
the  
silly  
little  
notification  
apps  
that  
wree  
brought  
up  
here  
as  
justification  
for  
allowing  
anybody  
to  
use

Re: Current status?

Re: Current status?

port  
25.  
They  
have  
no  
builtin  
method  
of  
authenticating  
so  
the  
port  
number  
used  
changes  
nothing.  
I  
certainly  
would  
not  
accept  
email  
on  
my  
MTA  
from  
someone  
on  
port  
587  
that  
I  
would  
not  
also  
accept  
on  
port  
25.  
The  
purpose  
of  
port  
587  
and  
RFC  
2476  
is  
not  
to  
control

Re: Current status?

Re: Current status?

SPAM  
it  
is  
to  
make  
sure  
outgoing  
email  
meets  
the  
proper  
formatting  
requirements  
of  
the  
other  
RFC's.

On  
the  
other  
hand  
MTAs  
talk  
to  
MUAs  
(when  
delivering  
mail)  
using  
either  
of  
2  
different  
protocols  
(that  
I  
know  
of),  
POP3  
on  
port  
110  
and  
IMAP  
on  
port  
143.  
(I

Re: Current status?

Re: Current status?

don't  
think  
anything  
does  
POP2  
on  
port  
109  
any  
more.)

Logically  
there  
are  
three  
parties  
involved  
not  
two.  
MTA,  
MUA  
and  
Message  
store.

Not  
sure  
what  
you  
make  
as  
differnt  
with  
"Message  
store".  
Unless  
you  
are  
separating  
the  
guy  
MTA  
from  
the  
machine  
that  
runs  
POP  
or

Re: Current status?

Re: Current status?

IMAP.  
I  
don't  
see  
that  
as  
necessarily  
being  
a  
separate  
Email  
function  
although  
it  
is  
possible  
and  
may  
even  
have  
some  
utility  
on  
a  
big  
enough  
system.

The  
MTA  
delivers  
mail  
to  
another  
MTA  
or  
to  
a  
message  
store.  
The  
MUA  
originates  
mail  
and  
sends  
it  
to  
a

Re: Current status?

Re: Current status?

MTA.  
Mail  
clients  
generally  
incorporate  
the  
above  
MUA  
functionality  
together  
with  
the  
ability  
to  
display  
and  
manipulate  
mail  
in  
the  
message  
store.

POP  
and  
IMAP  
are  
protocols  
used  
to  
access  
and  
manipulate  
the  
message  
store.  
They  
are  
NOT  
used  
to  
deliver  
mail  
to  
the  
message  
store.

Agreed,  
but

Re: Current status?

Re: Current status?

the  
"Message  
Store"  
is  
not  
necessarily  
even  
a  
part  
of  
the  
Email  
system  
and  
I  
don't  
believe  
it  
has  
ever  
been  
considered  
by  
IETF.  
I  
have  
users  
who  
use  
NFS  
to  
read  
their  
email.  
Does  
that  
make  
NFS  
an  
Email  
Protocol,  
too?  
And,  
of  
course,  
Wessage  
Store  
is  
also  
irrelevant  
to

Re: Current status?

Re: Current status?

the  
problem  
of  
how  
to  
get  
the  
email  
system  
to  
be  
more  
immune  
to  
SPAM.

Note.

The  
SMTP  
servers  
which  
come  
with  
the  
TCPIP  
stacks  
(TCPWARE,  
MULTINET  
or  
TCPIP  
SERVICES/UCX)  
are  
NOT  
fully  
fledged  
modern  
MTAs.  
For  
that  
you  
would  
need  
either  
PMDF  
or  
MX.  
(  
PMDF

Re: Current status?

Re: Current status?

is  
a  
commercial  
product  
but  
is  
available  
free  
for  
hobbyist  
use.  
MX  
is  
now  
an  
open-source  
free  
product  
see  
<http://www.madgoat.com/>  
However  
I'm  
not  
aware  
of  
anyone  
currently  
continuing  
development  
of  
MX.  
)

Maybe  
so,  
but  
if  
people  
played  
by  
the  
rules,  
basic  
SMTP  
is  
more  
than  
adequate  
to

Re: Current status?

Re: Current status?

the  
task.  
If  
ISP's  
blocked  
port  
25  
for  
all  
machines  
in  
their  
domain  
other  
than  
their  
MTA  
I  
would  
need  
to  
filter  
incoming  
ports  
on  
my  
end.  
And  
RBL's  
would  
rapidly  
become  
redundant.

Sadly,  
we  
are  
forced  
to  
spend  
a  
lot  
of  
time  
effort  
and  
technology  
trying  
to,  
once  
again,

Re: Current status?

Re: Current status?

solve  
a  
social  
problem.  
A  
social  
solution  
would  
work  
a  
lot  
better.

Perhaps  
it  
would.  
But  
where  
would  
you  
get  
a  
"social  
solution"?  
How  
would  
you  
implement  
it?  
How  
would  
you  
deal  
with  
the  
anti-social  
creeps  
who  
"zombie"  
a  
PC  
or  
two  
or  
twenty  
and  
use  
them  
to  
pump

Re: Current status?

Re: Current status?

spam  
into  
the  
net?  
Hint:  
you  
will  
NEVER  
get  
the  
liberals  
to  
agree  
to  
the  
death  
penalty!  
Hell,  
you  
can  
even  
spank  
a  
misbehaving  
child  
any  
longer!

Like I said,  
I have been  
over this a  
half-dozen  
times  
already. All  
that  
is needed  
already  
exists. It  
takes only  
administrative  
changes  
(which is  
why I said it  
would  
require  
more effort  
on the part  
of admins).  
If you  
are truly

Re: Current status?

Re: Current status?

interested,  
email me  
and I will  
explain it to  
you. Or, if  
others  
actually  
express  
interest I  
will post it  
here again.  
But I  
expect most  
here are not  
in the least  
bit  
interested.

bill

My ISP has a spam filter  
effective enough that spam  
is not a problem for  
me! I get the occasional  
"401 scam" but that's about  
all.

And how many messages have you not  
received because of their SPAM filter?  
False Positives are at least as bad a problem  
as False Negatives. And for  
a business, they can be worse.

If I did not receive a message, it's unlikely that I would be  
aware of  
it except if it came from family or friends and they inquired  
if I had  
received it or complained about my failure to reply.

Which is the point of the question. Aggressive SPAM filtering sounds nice,  
but how do you know the rate of False Positives? Answer: you don't.

Re: Current status?

I do get mail from PC Connection, CDW, HP, Amazon, and a few other commercial enterprises that I have some kind of relationship with. I don't consider it spam and don't complain about it.

Yes, but have you ever sent an email to a company and not received an expected answer? I know people who complained regularly that their emails to Mentec were ignored. But the fact is, you don't know if they ever arrived in the first place. How many businesses can afford to just blow off customers because of aggressive SPAM filtering?

Comcast does seem to block 99.9+% of the people selling penis enlargers, nude photographs, drugs without prescription, etc.

While willingly supporting a network infrastructure that inundates the INTERNET with that garbage even though it is bad engineering at best and deliberate at worst.

And, before you sing the praises of Comcast..... I just looked at my logs and I have several hundred rejected connection from comcast addresses and that is just since midnight.

My router blocks any and all connections that did not originate from my home network. If I check the router's logs, something I may do once or twice a year, there is somebody attempting a connection every fifteen to twenty seconds, twenty-four hours a day. Should I wish to receive incoming connections, I believe that I can configure it to allow specific originating addresses and ports but I can't think of any reason why I should want to. That box only cost me about \$80 US and it has paid for itself several times over!

Re: Current status?

Re: Current status?

Is this your home router? if it is, your ISP should never allow you to even see them. That's what their firewall is for. basically, you are paying for the infrastructure that provides the needed bandwidth for all this garbage. (Yes, even connection requests that get rejected consume bandwidth and CPU time that could be better spent doing real work!) Of course, if it's your business LAN then that's what your firewall is supposed to do. Now, if we could just get a lot of other people, Comcast among them to do this SPAM would just go away!!

bill

Even if an ISP blocks external port 25 (which their customers would probably complain about if they are running their own inbound mail servers,

Every ISP I am aware of has a "no servers" in their residential AUP. You did actually read the AUP before signing up with the ISP, right?

or just on principal :-), do any implement internal firewalls that block one customer from trying to access another?

What one Comcast customer does to another is their problem. When they let it out on the INTERNET, which they don't own, it's a different matter.

For Comcast in particular, if I understand it correctly, each neighborhood is a LAN on a virtual ethernet running on their cable, so there is not even a router between you and the guy down the street. The only place they could put a firewall is on the cable converter box that converts the cable signal to ethernet in your house (the box commonly called a "cable modem", though I don't think it is really a modem.)

See above.

They could \*also\* firewall port 25 at their boundaries with other ISPs and backbone providers, but that in itself would be insufficient. (They might want to do it anyway to reduce their internal traffic.)

How would it be insufficient? It would prevent all their zombied machines from sending crap to every address in the users addressbook

Re: Current status?

Re: Current status?

because they couldn't connect to them. You do know that's how at least 95% of the current SPAM is done, right?

I'm on Verizon FIOS at home and I know the FIOS converter box is a router and does NAT and some level of filtering, so inbound port 25 traffic wouldn't make it to my LAN (or single computer if that was all I had) unless I actively reconfigure it to pass port 25 to a designated host (the default is "block"), but I don't know if the same applies to Comcast cable modems. (FIOS is point-to-point to the central office, like DSL, so local "LAN" traffic isn't a separate issue like it would be with Comcast.) In other words, blocking at the upstream router or at my home would be equally effective with FIOS or DSL, but for Comcast, only blocking at the home would catch everything.

Inbound port 25 to your machine is not the source of SPAM, outbound from your machine, which has no business sending email to anyone but your local MTA for relaying, to the INTERNET in general is. It doesn't require blocking at the user level, just at the border of the email domain which is your ISP.

As far as making SPAM go away, most of mine seems to come from China, South America, and other places, and gets sent through the legitimate ISP inbound mail server.

Look up the addresses blocks sometime. They are zombied PC's just like here. If the Chinese or Brazilian ISP blocked them it, too, would go away. Some, especially from South America" is from sites that offer SPAM Services. Those are also easily blocked if they haven't already made one of the RBL's.

It would have to be blocked at all those remote ISP's which are completely out of control.

RBL's do that now. And some people (myself included) block others that are particular problems that have not been RBLed yet.

And blocking port 25 inbound through the ISP's perimeter to anything other than its MX-designated mail servers

Re: Current status?

Re: Current status?

You can't do it from the inbound side. That's why it requires the ISP's doing on their outbound side.

would still do nothing about compromised hosts or deliberate SPAMing by other customers of the same ISP going through its outbound and then inbound mail servers.

That would be the ISP's problem. As long as it does not affect the rest of the INTERNET it is up to them to solve their own problems. When they let it affect the rest of the INTERNET it is no longer just their problem and they have become bad net neighbors. Kind of like the guy who starts a pig farm next door to your house.

It would make the offending hosts identifiable, but wouldn't stop them. The ISP would have to notice and then take action (which many of them do, but they have to send several hundred emails before anything gets triggered.)

Actually, no they don't. all they have to do is stop issuing the offending customer an IP address. When they call about their service being down you tell them fix their system or expect termination for violation of the AUP.

The SPAMers don't care. If they get several hundred sent from each zombie before they get stopped, they're happy, and the rest of us suffer.

And if the ISP's blocked port 25 at their outbound firewall/router none of it would go anywhere because the zombied machines would get nothing but connection timeouts.

As far as liberals coddling SPAMers, I'm a liberal and I say "hang'em now. We can have the trial later!"

I never said anything about liberals. I said the problem is primarily incompetents. This isn't rocket science!!!

bill

Re: Current status?

Re: Current status?

—

Bill Gunshannon | de-moc-ra-cy (di mok' ra see) n. Three wolves  
billg999@xxxxxxxxxxxxxxxxx | and a sheep voting on what's for dinner.

University of Scranton |  
Scranton, Pennsylvania | #include <std.disclaimer.h>

.