

Re: Incoherent E-mails

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2005-10/0342.html>

From: Hairy One Kenobi (*abuse_at_[127.0.0.1]*)

Date: 10/20/05

Date: Thu, 20 Oct 2005 00:07:43 GMT

"Moe Trin" <ibuprofin@painkiller.example.tld> wrote in message news:slrndld917.6qc.ibuprofin@compton.phx.az.us...
> *In the Usenet newsgroup alt.computer.security, in article*
> *<Eaf5f.142\$65.118@newsfe6-win.ntli.net>, Hairy One Kenobi wrote:*
> *> "Moe Trin" <ibuprofin@painkiller.example.tld> wrote*
>
> *>> So I can complain about the stupidity of microsoft for including*
> *>> messenger without even rudimentary security precautions like TTL*
> *>> limits or (even better) using TCP instead of UDP*
>
> *>Haven't ["Don't" would be more accurate] use MSN-style stuff.*
>
> *As usual, microsoft didn't invent this function either. But then, neither*
> *did *nix.*

Or VMS (just to cut assumptions short, I'm not exactly young either, and have more than a decade programming VAXen). While I'm here, the obligatory

<much snippage>

Anyway. One of the best pranks we ever set up was to take-over terminals and use VT codes to duplicate system messages.

The Sysman fell for incoming email from NORTHPOLE::SANTA (twice!), but sussed-out that something was suspicious when he received a missive from HEAVEN::GOD ;o)

Chat was also used on occasion. Last OS that I used that /didn't/ have this facility was CP/M 3. MP/M 2 (i.e. the version that was supposed to), I *think* had it. Haven't used it since school, so I can't remember. The BBC (running on our own E*Net) had the functionality.

> *>TTL should be a function of the stack but, architecturally, UDP is*
> *>better suited – IMHO! – than TCP.*
>
> *Re TTL, yes it's network stack function, and if you look at the basics,*
> *several O/S (AIX, OSF/1, and Ultrix at least) used different TTLs for*

> *TCP versus UPD. Traceroute (and clones) directly mucks with TTL, and
> microsoft's gift to the MCSE who screws up the configuration of the
> DHCP server called 'link-local' or 'zero-conf' is not only required
> to have a TTL=1, but it's also not to be forwarded (RFC3927). DHCP and
> the older BOOTP were not supposed to be forwarded either (there are
> relay agents that would normally run on a router that are allowed to
> forward the requests/replies), and some multicasts (RFC1301) are also
> limited, often by TTL. The Novell crap was originally run on IPX
> (rather than IP), and it, like microsoft's original NETBEUI was not
> routable. I can't remember what Novell did when they ran IP rather
> than IPX – but they used a different type number as I recall (I don't
> think it was TCP/UDP/ICMP).*

Never really used IPX, but I seem to recall that it was very routable – just in the DECnet way (node-node).

They added a bastard creation by encapsulating IPX over IP, demonstrating how forcing fixed-size frames into variable packet lengths could do "interesting" things to networks. Remember, "proper" switches and routers were in their infancy, so packets would fly hither and thither, arriving in odd orders.

The term in the early-mid nineties was "packet storm". Just one machine jabbering could take down and appreciable chunk of infrastructure (been there, fixed that)

> *>It's a one-way stream of garb^H^H^H^information, followed by like.
>
> The original concept was to announce that the system was going to go
> down for this or that reason (don't forget, this was back when they
> were developing code, and many users could be logged in to a single
> computer), or that Snicker-Snacks had arrived in the break room or
> some-such. It's based on the much earlier TENEX 'LINKS' and 'NOTIFY'
> stuff from mid-late 1960s.*

And earlier. Hell, LEO undoubtedly had "your printer is jammed" messages ;o)

> *>No need for a handshake, either technically or (shudder)
metaphorically/in
> >person.
>
> Haven't tried 'talk' – have you? Full interactive text between users.
> But then, look at your shell's man page, and discover that most have a
> 'mesg' like command (Bourne derived shells) to ignore messages.*

Used, yes. Bothered-with on UNIX, no.

> *UDP is of lesser usefulness on the Internet. The only protocol that
> requires it is DNS – and if you didn't get the reply, you asked again,
> but with larger delays between requests, and a maximum of 3 per server.
> Sure, stuff like NFS uses UDP, but I haven't seen to many people*

- > *allowing mounts past a perimeter. The original advantage of UDP was*
- > *the lower overhead – the header is just 8 bytes, compared to 20 to*
- > *60 bytes for TCP. This was an advantage on bandwidth limiting links,*
- > *but cost some additional CPU time to compensate.*

Erm, not really. There are very valid uses for even lossy systems (SNMP, for example) – the main advantage is, when sending a small message, that you don't need the massive overhead of the handshake.

That's it, basically.

For streamed content (very common outside of UNIX clients ;o), the uber-protocol is happy to handle its own sequencing, so the TCP auto-resequence becomes nothing more than an overhead, both in terms of CPU, bandwidth and (more importantly) propagation/latency.

In other words, UDP is perfectly valid for a whole host of protocols for a whole host of sound engineering reasons.

- > *The simple advantage of TCP over UDP is the required 3-way handshake*
- > *before data transfer.*

The only thing you're checking is the IP address. Hardly a major hurdle, unless it's actually a legitimate machine, rather than something borked. In any event, who thehell has RPC exposed on a 'Net connection?!?

H1K