

comp.security.misc: Re: what if the message-ID generator generates a dirty word?

Re: what if the message-ID generator generates a dirty word?

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2002-01/0410.html>

From: Walter Roberson (roberson@ibd.nrc.ca)

Date: 01/22/02

From: roberson@ibd.nrc.ca (Walter Roberson)

Date: 22 Jan 2002 04:42:49 GMT

In article [<vxkwuybqs4z.fsf@cinnamon.vanillaknot.com>](mailto:vxkwuybqs4z.fsf@cinnamon.vanillaknot.com),

Karl Kleinpaste [<karl+usenet@charcoal.com>](mailto:karl+usenet@charcoal.com) wrote:

:Barry Margolin [<barmar@genuity.net>](mailto:barmar@genuity.net) writes:

:> How about all-numeric (or mostly-numeric, except for username and date

:> sections) message ID's?

:Why should anyone care, considering that the flaw is imaginary in practice?

The "flaw" -isn't- imaginary in practice. Your sample of 30K messages was just too small.

Each 4-letter word maps to a 4-digit (base 36) number, which is broken into a 16 bit time and a 1-in-25 selector. Thus there is a 1 in 1638400 chance of producing any particular four-letter word at random. We would have to designate 55 different "bad words" for there (on average) to be one hit in 30K messages. You were only searching on about 7, so there was only about 1/8th of a chance you'd find any.

Any site that generates enough IDs is likely to eventually create a match -- the question becomes what happens then?

Then there is the problem that the upper 16 bits of the time cannot be called random: half of all words will crop up for 18 hour windows.

According to my calculations, these should have shown up in the recent past:

leer: Random value (0..25) of 15; time 15411 starting from Wed Jan 2 12:41:36 2002

and soon to show up is this:

left: Random value (0..25) of 15; time 15449 starting from Thu Jan 31 08:27:44 2002

The previous year should have included these. Note in particular

Re: what if the message-ID generator generates a dirty word?

comp.security.misc: Re: what if the message-ID generator generates a dirty word?

the second of these.

sewn: Random value (0..25) of 20; time 14967 starting from Tue Jan 30 17:55:12 2001
sexy: Random value (0..25) of 20; time 15014 starting from Wed Mar 7 09:31:44 2001
plug: Random value (0..25) of 18; time 15064 starting from Sat Apr 14 07:45:04 2001
plum: Random value (0..25) of 18; time 15070 starting from Wed Apr 18 20:58:40 2001
plus: Random value (0..25) of 18; time 15076 starting from Mon Apr 23 10:12:16 2001
cyst: Random value (0..25) of 9; time 15149 starting from Sun Jun 17 19:07:44 2001
frye: Random value (0..25) of 11; time 15174 starting from Fri Jul 6 18:14:24 2001
eddy: Random value (0..25) of 10; time 15174 starting from Fri Jul 6 18:14:24 2001
eden: Random value (0..25) of 10; time 15199 starting from Wed Jul 25 17:21:04 2001
lead: Random value (0..25) of 15; time 15253 starting from Tue Sep 4 16:23:28 2001
leaf: Random value (0..25) of 15; time 15255 starting from Thu Sep 6 04:48:00 2001
leak: Random value (0..25) of 15; time 15260 starting from Sun Sep 9 23:49:20 2001
edge: Random value (0..25) of 10; time 15262 starting from Tue Sep 11 12:13:52 2001
lean: Random value (0..25) of 15; time 15263 starting from Wed Sep 12 06:26:08 2001
leap: Random value (0..25) of 15; time 15265 starting from Thu Sep 13 18:50:40 2001
lear: Random value (0..25) of 15; time 15267 starting from Sat Sep 15 07:15:12 2001
edgy: Random value (0..25) of 10; time 15282 starting from Wed Sep 26 16:19:12 2001
edit: Random value (0..25) of 10; time 15349 starting from Fri Nov 16 12:01:04 2001
leek: Random value (0..25) of 15; time 15404 starting from Fri Dec 28 05:15:44 2001

Try searching for 'sexy' in your store of IDs, if you were active on March 7th.

- ***Next message:*** Bernd Felsche: "Re: Schneier: Trust, but verify, Microsoft's pledge"
- ***Previous message:*** Walter Roberson: "Re: workstation attacks vs. server attacks"
- ***In reply to:*** Karl Kleinpaste: "Re: what if the message-ID generator generates a dirty word?"
- ***Next in thread:*** Jacques L'helgoualc'h: "Re: what if the message-ID generator generates a dirty word?"
- ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]