chgTDbuf

COLLABORATORS			
	TITLE : chgTDbuf		
ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY		January 7, 2023	

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

chgTDbuf

1.1 chgTDbuf v33 - Click'n'read table of contents...

```
                          ##             ###### ######   ##                  ↩
                             ###
         ##                  ##   ##   ##  ##                 ## ##
  ####   #####    ####   ##   ##   ##  #####   ##  ##   ##
##  ##  ##  ##  ##  ##  ##   ##   ##  ##  ##  ##  ##  ####
##      ##  ##  ##  ##  ##   ##   ##  ##  ##  ##  ##   ##
##  ##  ##  ##   #####  ##   ##   ##  ##  ##  ##  ##   ##
 ####   ##  ##      ##  ##   ######    ####    ####    ##
                  #####
Version 33.01
```


1.2 chgTDbuf v33 - About TrapDoor v1.83 and its bugs...

*** HOW I DID IT ***

First, I am talking about a patch to TrapDoor v1.83: the fidonet mailer by Maximilian Hantsch and Martin Laubach. If you don't own TD, this program will be useless for you.

I have to be a bit technical, sorry. If you do not understand something in this document try reading TrapDoor.Man and FidoNet.Man...

During some EMSI connection TD gurus, trying to increase the process' stack (as the program's manual states) has no success.
There are nodes that make TD guru and others not, commonly multi domain HUBs are the killers.

I looked up at FSC-0056 and I discovered that the EMSI_ISI (or EMSI_ICI) packets can't be longer than 2048 bytes, so I looked inside the binaries of TD to see if this was the cause of my gurus. TD breaks the ISI fields and examines each field using a temporary 520 bytes long buffer, and this in normal operation environment should be enough...

I also read on TD manual that there is a limit of 20 AKAs for the system. Each address (i.e. 32767:32767/32767.32767@mydomain.foo) may be up to 36 bytes long, 20*36 is a number bigger than 520 (don't forget brackets and separators): let's say about 758 bytes?
Now, what about a HUB with more than 20 AKAs?

TD was written in C, and naturally the packet parser is a function.
Automatic variables (and arrays) are put just below the stack by the complier, so if the program copies too many data in this buffer it will overwrite, first the return address of the calling function, then the current function parameters, then the parameters and the return addresses of other functions. This means the program will crash trying to exit the function.

My fix is quite simple: I increase the temporary buffer size so "important" values stored on the stack will not be overwritten anymore.

TD still has the limit of 20 AKAs, the only improvement is that your system won't crash if the node you are calling has a too long AKAs string.

1.3 chgTDbuf v33 - Yes, I'm a lawbreaker (Robin Hood)

*** THOU SHALT NOT REVERSE ENGINEER ***

Open TD manual at page 73, and read chapter 11.3.7 (License).
Got it? I cannot disassemble the program.

But don't ask me why *I* had to fix the bug instead of the authors!

As far as I know Max & Martin received the bug report via crashmail, they were also invited to leave simple hold replies on their node, they were polled everyday for 15 days from Italy without getting a reply.

Keep in mind that fixing the bug needs no more than 5 minutes, but they seem to have other to do...

*** FIDONET STARRING ***

Giancarlo "Vertigo" Cairella ..... sysop on BBS2000 2:331/301
owner of a node with more than 20 akas
Thanks! you replied to my testing crashmail

Luca Mirabelli ..... pointop on 2:331/301.5
unhappy registered user which called
for 15 days the TD support site without
getting a reply
Thanks! you spotted me the problem making my life easier

Nicola "O'Patchatore" Soggia ..... pointop on 2:331/315.3
the registered user #14320 who broke
the license to bugfix the program for
free
Thanks! you bugfixed the program (let's hope)

Gian! Salerno ..... sysop on TiTanic 2:331/315
betatester of the patched version
Thanks! you let your node crash for me

Paolo Maggi ..... pointop on 2:331/315.9
betatester of the patched version
Thanks! you crashed Gian!'s node for me ;-D

1.4 chgTDbuf v33 - User's manual

*** EXECUTING THE PROGRAM ***

chgTDbuf can be run either from CLI/Shell or Workbench under any Kickstart, and it needs no arguments or tooltypes.
If all goes ok, a window with some gadget should appear, otherwise the screen will flash as intuition is not able to open the window (Is the Workbench screen big enough? Is there enough memory?).
If the program exits immediately without flashing it is because it is not able to open dos and intuition libraries, this should never happen tho.

*** GRAPHICAL USER INTERFACE ***

WINDOW CLOSE GADGET
Click once on this gadget to quit immediately the program (no confirmation will be asked).

"SOURCE" STRING GADGET
Type here the source file name, the original file to be read and patched. If you enter nothing the destination string gadget contents will be cloned here.

"DESTINATION" STRING GADGET
Type here the destination file name, the new file to be created from the patched one. If you enter nothing the source string gadget contents will be cloned here.

"GET..." GADGETS
Let you fill the corresponding string gadget with a file name selected with a standard asl file requester.
The program tries to open the asl.library on startup, if the library isn't available these gadget will be ghosted (this means that no file requesters are available under kickstart 1.2 and 1.3).
In very low memory situations clicking on a "Get..." gadget will simply make the screen flash instead of opening the file requester.

"EMSI BUFFER" INTEGER STRING GADGET
Lets you choose the new buffer size (original TrapDoor size is 524, my default size is 2048).
Valid range is 524 to 32768 in steps of 4 (don't worry: all is automagic).
If you enter an empty string, 2048 will be entered for you.
If you type 0, the size will be the one of the source file, or 524 if the source file doesn't exist or it is not TD 1.83.
This is the most dangerous of the gadgets, because too small values may not be enough not to overwrite "important" data, and too big values may crash your Amiga if there's no enough stack available.
The program lets you enter numbers up to 32768, but please never enter values bigger than 8192, use big values for debugging purposes only.

ALWAYS REMEMBER: if you increase the buffer you will need enough stack room to put your data, you cannot use i.e. a 8Kb buffer if you have only 4Kb for the stack. Please be sure that the process stack size is always at least 4 or 6 Kb bigger than the new buffer size (and if this is still not enough raise the stack).
Unfortunately TD doesn't check if the stack is big enough before allocating its variables (see pages 33 and 68 of the TD user's manual), and if there is not enough room it will much probably hang your Amiga.

"PATCH AND SAVE" GADGET
Click on this gadget when you think that source, destination and buffer size are set as you want. This will create a patched TD file.

*** INFORMATION BOX ***

This box lets you know what probably will happen if you click on "Patch and save" gadget, it contains three sub-fields (or lines).

the first subfield is updated when you enter (by hand or by the file requester) the source filename

SOURCE: NOT A FILE (IT'S A DRAWER)
you selected as source a drawer or a volume.
if the filename is missing the source can't be opened

SOURCE: READ PROTECTED
you selected as source a read protected td 1.83 file.
this is not harmful, but you can't see the source buffer size

SOURCE: DOESN'T EXIST
you selected as source a file that doesn't exist.
if the file is missing it can't be opened

SOURCE: WRONG FILE (TOO SHORT)
you selected as source a file shorter than 105664 bytes.
this is not a original td 1.83 file and can't be patched
(probably you crunched the file, try decrunching it)

SOURCE: WRONG FILE (TOO LONG)
you selected as source a file longer than 105664 bytes.
this is not a original td 1.83 file and can't be patched

SOURCE: WRONG (OR MANGLED) FILE
you selected as source a 105664 bytes long file but it is not td 1.83.
this is not a original td 1.83 file and can't be patched

SOURCE: TRAPDOOR 1.83 (BUFFER: ????)
you selected as source a valid (non read protected) td 1.83 file.
the file can be read, patched, and re-saved.

the second subfield is updated when you enter (by hand or by the file requester) the destination filename

DESTINATION: NOT A FILE (IT'S A DRAWER)
you selected as destination a drawer or a volume.
if the filename is missing the destination can't be opened

DESTINATION: WRITE AND/OR DELETE PROTECTED
you selected as destination a write and/or delete protected file.
this file can't be overwritten, so destination can't be created

DESTINATION: DOESN'T EXIST
the file you selected as destination doesn't exist.
when you decide to save the destination it will be newly created

DESTINATION: ALREADY EXISTS
the file you selected as destination exists.
when you decide to save the destination file the previously data stored in that file will be lost

the third subfield is updated when you enter (by hand or by the file requester) the source or the destination filename

INFORMATION: READY

```
(kick 1.2/1.3 only) the source file is valid.
you can click on "patch and save" to create the destination file

INFORMATION: NOT READY
(kick 1.2/1.3 only) the source file is not valid.
if you click on "patch and save" the destination file will not be created

INFORMATION: DESTINATION IS NOT THE SOURCE
(kick 2.0/3.0 only) the destination file will not overwrite the source.
when you click on "patch and save" you preserve the original file

INFORMATION: DESTINATION IS THE SOURCE
(kick 2.0/3.0 only) the destination file will overwrite the source one.
when you click on "patch and save" you loose the original file


when  you  click  on "patch and save" the third field will contain a error
report (which will stay up until you select any file)


INFORMATION: CAN'T OPEN SOURCE
missing volume, missing file, file protected or illegal name.
change name or check volume.

INFORMATION: CAN'T READ FROM SOURCE
missing volume, corrupted volume or not a td 1.83 file.
check file and volume.

INFORMATION: CAN'T OPEN DESTINATION
missing  volume,  volume  write  protected, volume full, file protected or
illegal name.
change name or check volume.

INFORMATION: CAN'T WRITE TO DESTINATION
volume  ejected,  volume  full  or  illegal name (destination file will be
erased if possible).
check volume.

INFORMATION: PLEASE CHANGE THE EMSI BUFFER
the program never creates a destination file equal to the source one.
enter another emsi buffer size.

INFORMATION: TRAPDOOR HAS BEEN PATCHED
operation was successful.
select other files, buffer sizes or quit program.
```

1.5 chgTDbuf v33 - I have better things to do by night!

*** SECURITY ***

```
Unless  you  have up/downlinks who have a too long aka string, there is no
why for you to install the buffer patch.
Anyway, if you installed the patch and want to remove it, just set the emsi
buffer to 524 and you'll get the original binaries.
```

*** PARANOID ***

Now you are thinking that it is possible that the archive you downloaded has been tampered. I hatched it in SAN, so if you downloaded the archive directly from a Sky Amiga Network node there should be no problems at all (I know, the node's sysop may have tampered the archive...).

You can check the destination binaries by hand (use a hex calculator to find the correct 16 bit buffer size). Here follows a "type opt h" dump of the binaries. ---- marks show where the file is patched by chgTDbuf.
If you find other differences, the program has been tampered.

```
2970: 4E55---- 48E70330 2E002C01 26482B49    NU--Hç.0..,.&H+I
2980: ----7001 2B40FFF8 6050101B B0076646    --p.+@.ø‘P..\textdegree{}.fF
2990: 45ED---- 60224A13 6722204A 528A224B    Eí--`"J.g" JR."K
29A0: 6100FF6E 26401013 B00666EA 528B1013    a..n&@..\textdegree{}.fêR...
29B0: B0066608 14C6528B 4A1366EA 4212486D    \textdegree{}.f..ÆR.J.fêB.Hm
29C0: ----486D FFF8206D ----4E90 504F4A40    --Hm.ø m--N.POJ@
```

offset	original	patched
$2972	$FDF4	-bufsize
$2980	$FDF4	-bufsize
$2992	$FDF8	-bufsize+4
$29C0	$FDF8	-bufsize+4
$29C8	$FDF4	-bufsize

1.6 chgTDbuf v33 - Nicola Soggia (yes, Nicola is my first name ;-)

*** AUTHOR ***

If you have any suggestions, bug reports, or wish to let me know something about the package feel free to contact me at the E-Mail addresses below.

Fidonet.org: Nicola Soggia (2:331/315.3)
Amiganet.ftn: Nicola Soggia (39:101/102.3)
Internet/Arpa: Nicola.Soggia@p3.f315.n331.z2.fidonet.org
Usenet/Sublink: Nicola.Soggia@SkyLink.sublink.org

1.7 chgTDbuf v33 - FRED FISH, 345 Scottsdale road, Pleasant Hill, CA 94523

*** DISTRIBUTION ***

This package is released under the concept of freeware, the package must be distributed as one whole. The distributor may charge a fee up to the cost of the medium for the entire package.
This package can be included with commercial distributions without written

permission from the author.

*** DISCLAIMER ***

This package is provided as is, without warranty of any kind, either expressed or implied.
Should the package prove defective, you assume the entire cost of all necessary servicing, repair or correction even if I have been advised of the possibility of such damages.
I’m not responsible of the results of the use of the package.