kernelslacker / trinity

Linux system call fuzzer

5,077 commits | **1** branch | **8** releases | **45** contributors | GPL-2.0

Branch: **master** ▾ | **New pull request** | **Create new file** | **Upload files** | **Find file** | **Clone or download** ▾

kernelslacker Fix up null ptr deref when no -l arg.		Latest commit `14e3dbf` 6 days ago
.deps	Rework the dependancy generation.	5 years ago
Documentation	add hashcheck use to TODO	11 days ago
childops	move the 'are we done' check to the generic child code.	3 months ago
fds	make ->dump silent when running with -q	5 months ago
include	reinstate the log-to-file code for now.	20 days ago
ioctls	fix includes	a month ago
mm	convert map dump to use init_msgobjhdr	6 months ago
net	proto-rds: fix missing includes	23 days ago
patches	refresh patches	2 years ago
rand	replace __WORDSIZE with WORD_BIT	a month ago
scripts	add a script I use to monitor when the kernel interfaces change	11 days ago
server	output a packet count for debugging	23 days ago
syscalls	fix includes	a month ago
tools	update netlink protocols	3 months ago
.gitignore	generate the version string at make time, instead of configure time.	3 years ago
COPYING	Fix the header. oops.	5 years ago
Makefile	Fix version.h generation	a month ago
README	update some documentation regarding logging	11 days ago
arg-decoder.c	log.c->output.c log.h->arg-decoder.h	7 months ago
blockdevs.c	nr_blockdevs can't be negative	2 years ago
child.c	reinstate the log-to-file code for now.	20 days ago
configure	ipx: make optional	a month ago
debug.c	reinstate the log-to-file code for now.	20 days ago
devices.c	move output() and friends to trinity.h	7 months ago
ftrace.c	fix some ftrace resource leaks	6 months ago
generate-args.c	make iovec's with a single element half the time	7 months ago
kcov.c	Add initial support for kcov functionality.	a year ago
locks.c	don't spin on locks if we've already finished.	5 months ago
log-files.c	Fix up null ptr deref when no -l arg.	6 days ago
log.c	reinstate the log-to-file code for now.	20 days ago
main.c	reinstate the log-to-file code for now.	20 days ago
objects.c	copy the ->dump method into the child object header	5 months ago
output.c	make output() aware that LOGGING_UDP is a thing	11 days ago
params.c	update some documentation regarding logging	11 days ago
pathnames.c	pathnames: add missing nftw defines	a month ago
pids.c	fix off-by-one in dump_childnos()	6 months ago

post-mortem.c	move output() and friends to trinity.h	7 months ago
results.c	remove duplicate get_argval function	a year ago
shm.c	reinstate the log-to-file code for now.	20 days ago
signals.c	pass the signal from the sighandler using siglongjmp instead of globa…	a year ago
stats.c	move output() and friends to trinity.h	7 months ago
syscall.c	syscall: ensure a child is not killed with a lock held	a month ago
sysv-shm.c	remove a bunch of bogus __unused__ attributes	5 months ago
tables-biarch.c	remove old debug leftover	4 months ago
tables-uniarch.c	fix memory corruption in tables-uniarch:log_enabled_syscalls_uniarch	5 months ago
tables.c	get_syscall_entry: remove SYSCALL_OFFSET	3 months ago
taint.c	micro-optimize the 'became tainted' case.	6 months ago
trinity.1	update some documentation regarding logging	11 days ago
trinity.c	reinstate the log-to-file code for now.	20 days ago
udp.c	reinstate the log-to-file code for now.	20 days ago
uid.c	move output() and friends to trinity.h	7 months ago
utils.c	move output() and friends to trinity.h	7 months ago

README

```
Trinity: Linux system call fuzzer.

        "After the initial euphoria of witnessing the explosion had passed, test
         director Kenneth Bainbridge commented to Los Alamos director J. Robert
         Oppenheimer, "Now we are all sons of bitches."   Oppenheimer later stated
         that while watching the test he was reminded of a line from the Hindu
         scripture the Bhagavad Gita:

                Now I am become Death, the destroyer of worlds."


#######################################################################

WARNINGS:
* This program may seriously corrupt your files, including any of those
  that may be writable on mounted network file shares.  It may create network
  packets that may cause disruption on your local network.

* Trinity may generate the right selection of syscalls to start sending random network
  packets to other hosts. While every effort is made to restrict this to IP addresses
  on local lans, multicast & broadcast, care should be taken to not allow the
  packets it generates to go out onto the internet.

  Run at your own risk.


#######################################################################

System call fuzzers aren't a particularly new idea.   As far back as 1991,
people have written apps that bomb syscall inputs with garbage data,
that have had a variety of success in crashing assorted operating systems.

After fixing the obvious dumb bugs however, a majority of the time
these calls will just by rejected by the kernel very near the beginning
of their function entry point as basic parameter validation is performed.

Trinity is a system call fuzzer which employs some techniques to
pass semi-intelligent arguments to the syscalls being called.
```

```
The intelligence features include:

- If a system call expects a certain datatype as an argument
  (for example a file descriptor) it gets passed one.
  This is the reason for the slow initial startup, as it generates a
  list of fd's of files it can read from /sys, /proc and /dev
  and then supplements this with fd's for various network protocol sockets.
  (Information on which protocols succeed/fail is cached on the first run,
   greatly increasing the speed of subsequent runs).

- If a system call only accepts certain values as an argument,
  (for example a 'flags' field), trinity has a list of all the valid
  flags that may be passed.
  Just to throw a spanner in the works, occasionally, it will bitflip
  one of the flags, just to make things more interesting.

- If a system call only takes a range of values, the random value
  passed is biased to usually fit within that range.


Trinity logs it's output to a files (1 for each child process), and fsync's
the files before it actually makes the system call. This way, should you trigger
something which panics the kernel, you should be able to find out exactly what
happened by examining the log.

There are several test harnesses provided (test-*.sh), which run trinity in
various modes and takes care of things like cpu affinity, and makes sure it runs from the
tmp directory. (Handy for cleaning up any garbage named files; just rm -rf tmp afterwards)

######### options ###############################################

 --quiet/-q: reduce verbosity.
   Specify once to not output register values, or twice to also suppress syscall count.

 --verbose: increase verbosity.

 -D: Debug mode.
     This is useful for catching core dumps if trinity is segfaulting, as by default
     the child processes ignore those signals.

 -sN: use N as random seed.  (Omitting this uses time of day as a seed).
  Note: There are currently a few bugs that mean no two runs are necessary 100%
  identical with the same seed. See the TODO for details.

 --kernel_taint/-T: controls which kernel taint flags should be considered.
        The following flag names are supported: PROPRIETARY_MODULE, FORCED_MODULE, UNSAFE_SMP,
        FORCED_RMMOD, MACHINE_CHECK, BAD_PAGE, USER, DIE, OVERRIDDEN_ACPI_TABLE, WARN, CRAP,
        FIRMWARE_WORKAROUND, and OOT_MODULE. For instance, to set trinity to monitor only BAD,
        WARN and MACHINE_CHECK flags one should specify "-T BAD,WARN,MACHINE_CHECK" parameter.

 --list/-L: list known syscalls and their offsets

 --proto/-P: For network sockets, only use a specific packet family.

 --victims/-V: Victim file/dirs.  By default, on startup trinity tree-walks /dev, /sys and /proc.
     Using this option you can specify a different path.
     (Currently limited to just one path)

 -p: Pause after making a syscall

 --children/-C: Number of child processes.

 -x: Exclude a syscall from being called.  Useful when there's a known kernel bug
     you keep hitting that you want to avoid.
     Can be specified multiple times.

 -cN: do syscall N with random inputs.
```

```
     Good for concentrating on a certain syscall, if for eg, you just added one.
     Can be specified multiple times.

 --group/-g
   Used to specify enabling a group of syscalls. Current groups defined are 'vm' and 'vfs'.

 --logging/-l <arg>
  off: This disables logging to files. Useful if you have a serial console, though you
         will likely lose any information about what system call was being called,
         what maps got set up etc. Does make things go considerably faster however,
         as it no longer fsync()'s after every syscall
  <hostname> : sends packets over udp to a trinity server running on another host.
         Note: Still in development. Enabling this feature disables log-to-file.
  <dir> : Specify a directory where trinity will dump its log files.

 --ioctls/-I will dump all available ioctls.

 --arch/-a Explicit selection of 32 or 64 bit variant of system calls.

########################################################################

Examples:
./trinity -c splice
Stress test the splice syscall

./trinity -x splice
Call every syscall except for splice.

./trinity -qq -l off -C16
Turn off logging, and suppress most output to run as fast as possible. Use 16 child processes


########################################################################

Development discussion of trinity occurs at trinity@vger.kernel.org
As with all vger mailing lists, subscribe by sending 'subscribe trinity'
in the body of a mail to majordomo@vger.kernel.org

######### Links to similar projects #####################################

= tsys - 1991.
  http://groups.google.com/groups?q=syscall+crashme&hl=en&lr=&ie=UTF-8&selm=1991Sep20.232550.5013%40smsc.sony.com&rnum=1

= iknowthis
  http://iknowthis.googlecode.com
  Fuzzer by Tavis Ormandy with very similar goals to this project.

= sysfuzz
  basic fuzzer by Ilja van Sprundel
  mentioned in http://events.ccc.de/congress/2005/fahrplan/attachments/683-slides_fuzzing.pdf
  http://leetupload.com/dbindex2/index.php?dir=Linux/&file=sysfuzz.tar.gz

= xnufuzz
  https://github.com/fintler/xnufuzz/tree/
  basic fuzzer for XNU.  Looks to be based on Ilja's sysfuzz.

= kg_crashme / ak_crashme / dj_crashme
  Kurt Garloff wrote a fuzzer similar to Ilja's sysfuzz in 2003.
  The ak / dj variants were improvements added by Andi Kleen, and Dave Jones.
```