

# dazuko: on access file system monitor

by eqmcc

dazuko: on access file system monitor.....	1
Description .....	2
Data structures .....	5
Test case .....	5
compile and install dazuko .....	5
test.....	7
The call flow.....	8

## Description

1. about dazuko(quoted from <http://dazuko.dnsalias.org/wiki/index.php/About>)

This Dazuko project provides a virtual device driver allowing (userland) applications to execute online file access control. It was originally developed by Avira GmbH (formerly known as H+BEDV Datentechnik GmbH) to allow on-access virus scanning. Other uses include a file-access monitor/logger or external security tools.

Dazuko operates by intercepting file access calls and passing the file information to a userland application. The application then has the opportunity to tell the virtual device driver to allow or deny the file access. The application also receives information about the file access event, such as accessed file name, type of access, process id, and user id.

2. dazuko and DazukoFS is not used in clamav any more:

<http://lists.nongnu.org/archive/html/dazuko-help/2010-10/msg00002.html>

### Re: [Dazuko-help] It is dead?

---

**From:** Frans de Boer  
**Subject:** Re: [Dazuko-help] It is dead?  
**Date:** Wed, 13 Oct 2010 20:22:05 +0200  
**User-agent:** Mozilla/5.0 (X11; U; Linux x86\_64; en-US; rv:1.9.1.12)


---

On 10/13/2010 10:41 AM, John Ogness wrote:  
> *Note: This email is being cross-posted to dazuko-devel since it*  
> *contains relevant development information.*  
>  
> On 2010-10-13, Frans de Boer <address@hidden> wrote:  
>  
>> *No progress, no resolution for the 2.6.35+ kernel...is there a*  
>> *change it will spark back to life or am I missing something?*  
>>  
> *The 2.6.36 kernel is about to be released. I don't plan on integrating*  
> *the already publicly available DazukoFS patches into a new version*  
> *until then. At that point I would also fix any new issues with 2.6.36.*  
>  
> *2.6.36 is actually a very interesting kernel release because it will*  
> *include (for the first time) the fanotify interface. Although the*  
> *implementation is quite different, fanotify could be used as a*  
> *replacement for DazukoFS. And since it is now mainline Linux, one must*  
> *ask if DazukoFS should continue to exist.*  
>  
> *I plan on writing test applications using fanotify to demonstrate that*  
> *fanotify can be a replacement for DazukoFS. If the applications indeed*  
> *show this (which I assume they will), then I will officially orphan*  
> *(or pass on maintenance of) DazukoFS (after fixing 2.6.36 issues).*  
>  
> John Ogness  
>  
>  
I know that ClamAV in the 0.97 release plan to use Fanotify instead of dazukoFS. When a product has made it main stream, then why try to continue if dazukoFS already has offered itself for inclusion in the main stream. As far as I know, it did not even made it into the staging area.

Anyhow, thanks sofar for given us dazuko and dazukoFS in the past.

Regards, Frans.

Note:  
the support of dazuko/dazukoFS is lifted from version 0.98 using fanotify(fan.c):

PUBLIC  vrtadmin / clamav-devel

Unwatch 43 13

Code Network Pull Requests 0 Issues 0 Wiki Graphs

ClamAV Development

Clone in Windows ZIP HTTP SSH Git Read-Only <https://github.com/vrtadmin/clamav-devel.git> Read-Only access


branch: master Files Commits Branches 14 Tags 133

clamav-devel / clamd / History

bb6578 - Fixes TODO in session.c on converting to ENUM  
lattera authored 4 months ago latest commit 8b2bde1b28

gitignore	4 years ago	update ignore files [aCaB]
Doxyfile	a year ago	Finish off documentation config files. [amishHammer]
Makefile.am	2 years ago	add fan.h to Makefile [Tomasz Kojm]
Makefile.in	6 months ago	Revert "Fix autotools on FreeBSD" [lattera]
clamd.c	4 months ago	bb6093 - check return value of fcntl [lattera]
fan-syscallib.h	2 years ago	clamd: initial support for on-access scanner using fanotify (bb#2236) [Tomasz Kojm]
fan.c	9 months ago	check of the return code from fstat() bb#5795 [Steve Morgan]
fan.h	2 years ago	clamd: initial support for on-access scanner using fanotify (bb#2236) [Tomasz Kojm]
localserv.c	11 months ago	BB#3737 - Value too large for specified data type [lattera]
localserv.h	4 years ago	update old copyright headers [Tomasz Kojm]
others.c	11 months ago	BB#3737 - Value too large for specified data type [lattera]
others.h	2 years ago	clamd: initial support for on-access scanner using fanotify (bb#2236) [Tomasz Kojm]
scanner.c	4 months ago	bb6082 - Fix compiler warnings [lattera]
scanner.h	4 months ago	bb6578 - Fixes TODO in session.c on converting to ENUM [lattera]
server-th.c	4 months ago	Coverity: don't kill a thread that was not created [Steve Morgan]

however in version 0.97.8, the clamuko is still there supporting dazuko/dazukoFS:

PUBLIC  vrtadmin / clamav-devel

Unwatch 43 13

Code Network Pull Requests 0 Issues 0 Wiki Graphs

ClamAV Development

Clone in Windows ZIP HTTP SSH Git Read-Only <https://github.com/vrtadmin/clamav-devel.git> Read-Only access

tag: clamav-0.97.8 Files Commits Branches 14 Tags 133

clamav-devel / clamd / History

Bumped FLEVEL, REVISION and Version string. Also modified NEWS and [kpyke]  
kpyke authored 4 months ago latest commit 392d5a93bb

gitignore	4 years ago	update ignore files [aCaB]
Makefile.am	4 years ago	removed r_gethostbyname which was not used [aCaB]
Makefile.in	4 months ago	Bumped FLEVEL, REVISION and Version string. Also modified NEWS and [kpyke]
clamd.c	2 years ago	clamd: fix log message verbosity [Török Edwin]
clamuko.c	a year ago	clamd: add support for on-access scanning on OS X with ClamAuth (beta) [Tomasz Kojm]
clamuko.h	a year ago	fix compile error [Tomasz Kojm]
clamukofs.c	2 years ago	clamd: add new option ClamukoExcludeUID (bb#2260) [Tomasz Kojm]
clamukofs.h	2 years ago	cosmetics (bb#2207) [Tomasz Kojm]
dazuko_xp.h	6 years ago	remove old CVS-stuff and make the repository look more like SVN [Sven Strickroth]
dazukoofs.c	4 years ago	clamd: add support for DazukoFS (bb#1691) [Tomasz Kojm]
dazukoofs.h	4 years ago	clamd: add support for DazukoFS (bb#1691) [Tomasz Kojm]
dazukoio.c	5 years ago	cosmetics [Tomasz Kojm]
dazukoio.h	6 years ago	remove old CVS-stuff and make the repository look more like SVN [Sven Strickroth]
dazukoio_compat12.c	5 years ago	improve handling of PDF, CAB, RTF, OLE2 and HTML files (sync with bra... [Tomasz Kojm]
dazukoio_compat12.h	6 years ago	remove old CVS-stuff and make the repository look more like SVN [Sven Strickroth]

strange enough in clamav-dev repository in git hub, the version 0.97.2 is still supporting dazuko:

PUBLIC vrtadmin / clamav-devel

Unwatch 0 Unstar 43 Fork 13

Code Network Pull Requests 0 Issues 0 Wiki Graphs

ClamAV Development

Clone in Windows ZIP HTTP SSH Git Read-Only <https://github.com/vrtadmin/clamav-devel.git> Read-Only access

tag clamav.0.97.2 Files Commits Branches 14 Tags 133

clamav-devel / clamd / History

bump numbers  
Tomasz Kojm authored 2 years ago latest commit 841fe231b2

..		
gitignore	4 years ago	update ignore files [aCaB]
Makefile.am	4 years ago	removed r_gethostbyname which was not used [aCaB]
Makefile.in	2 years ago	bump numbers [Tomasz Kojm]
clamd.c	2 years ago	cosmetics (bb#2207) [Tomasz Kojm]
clamuko.c	2 years ago	clamd: add new option ClamukoExcludeUID (bb#2260) [Tomasz Kojm]
clamuko.h	4 years ago	update old copyright headers [Tomasz Kojm]
clamukofs.c	2 years ago	clamd: add new option ClamukoExcludeUID (bb#2260) [Tomasz Kojm]
clamukofs.h	2 years ago	cosmetics (bb#2207) [Tomasz Kojm]
dazuko_xp.h	6 years ago	remove old CVS-stuff and make the repository look more like SVN [Sven Strickroth]
dazukoofs.c	4 years ago	clamd: add support for DazukoFS (bb#1691) [Tomasz Kojm]
dazukoofs.h	4 years ago	clamd: add support for DazukoFS (bb#1691) [Tomasz Kojm]
dazukoio.c	5 years ago	cosmetics [Tomasz Kojm]
dazukoio.h	6 years ago	remove old CVS-stuff and make the repository look more like SVN [Sven Strickroth]
dazukoio_compat12.c	5 years ago	improve handling of PDF, CAB, RTF, OLE2 and HTML files (sync with bra... [Tomasz Kojm]
dazukoio_compat12.h	6 years ago	remove old CVS-stuff and make the repository look more like SVN [Sven Strickroth]

while a version downloaded in Dec 2012 is surprisingly supporting fanotify already:  
see:

[https://github.com/eqmcc/clamav\\_decode](https://github.com/eqmcc/clamav_decode)

PUBLIC eqmcc / clamav\_decode

Pull Request Watch 0 Star 0 Fork 0

Code Network Pull Requests 0 Issues 0 Wiki Graphs Settings

clamav source code with comments

Clone in Windows ZIP HTTP SSH Git Read-Only [git@github.com:eqmcc/clamav\\_decode.git](git@github.com:eqmcc/clamav_decode.git) Read-Write access

branch: master Files Commits Branches 10 Tags

clamav\_decode / clamd / History

remove object files  
eqmcc authored 6 months ago latest commit 53ea040403

..		
gitignore	6 months ago	init [eqmcc]
Doxyfile	6 months ago	init [eqmcc]
Makefile.am	6 months ago	init [eqmcc]
Makefile.in	6 months ago	init [eqmcc]
clamd.c	6 months ago	init [eqmcc]
fan-syscallib.h	6 months ago	init [eqmcc]
fan.c	6 months ago	init [eqmcc]
fan.h	6 months ago	init [eqmcc]
localserver.c	6 months ago	init [eqmcc]
localserver.h	6 months ago	init [eqmcc]
others.c	6 months ago	init [eqmcc]
others.h	6 months ago	init [eqmcc]
scanner.c	6 months ago	init [eqmcc]
scanner.h	6 months ago	init [eqmcc]

## Data structures

TBD

## Test case

TBD

## compile and install dazuko

### environment:

#### OS

Ubuntu 7.04(kernel version: 2.6.20-15) PC (Intel x86) desktop @ <http://old-releases.ubuntu.com/releases/7.04/>

#### dazuko

<http://dazuko.dnsalias.org/files/dazuko-2.3.9.tar.gz>

### preparation

change apt source to legacy ones as bellow in /etc/apt/sources.list:

```
deb http://old-releases.ubuntu.com/ubuntu/ feisty main restricted universe multiverse
deb http://old-releases.ubuntu.com/ubuntu/ feisty-updates main restricted universe multiverse
deb http://old-releases.ubuntu.com/ubuntu/ feisty-security main restricted universe multiverse
deb http://old-releases.ubuntu.com/ubuntu/ feisty-backports main restricted universe multiverse
deb-src http://old-releases.ubuntu.com/ubuntu/ feisty-backports main restricted universe multiverse
```

update the data base:

```
sudo apt-get update
```

install openssh-server

```
sudo apt-get install openssh-server
```

get dazuko source files:

```
wget http://dazuko.dnsalias.org/files/dazuko-2.3.9.tar.gz
```

### Dazuko 2.3.9 (legacy stable)

Target	Type	File
(any of the following) <a href="#">RedirFS 0.8</a> Linux 2.2.0 - 2.6.22 <a href="#">Linux/RSBAC</a> <a href="#">FreeBSD 4 - 8</a>	kernel module <a href="#">CHANGELOG</a>	<a href="#">dazuko-2.3.9.tar.gz</a> <a href="#">[MD5]</a> <a href="#">[GPG]</a> 203 kB 19 Mar 2011

### check gcc version

```
gcc -v
Using built-in specs.
Target: i486-linux-gnu
Configured with: ../src/configure -v --enable-languages=c,c++,fortran,objc,obj-c++,treelang --prefix=/usr --enable-shared
--with-system-zlib --libexecdir=/usr/lib --without-included-gettext --enable-threads=posix --enable-nls --program-suffix=-4.1
--enable-__cxa_atexit --enable-clocale=gnu --enable-libstdcxx-debug --enable-mpfr --enable-checking=release i486-linux-gnu
Thread model: posix
gcc version 4.1.2 (Ubuntu 4.1.2-0ubuntu4)
```

### check kernel version and compiler

```
cat /proc/version
Linux version 2.6.20-15-generic (root@palmer) (gcc version 4.1.2 (Ubuntu 4.1.2-0ubuntu4)) #2 SMP Sun Apr 15 07:36:31 UTC
2007
```

### install kernel source, head files and g++

```
sudo apt-get install linux-source-2.6.20 linux-headers-2.6.20-15-generic g++-4.1
```

## compile

### compile dazuko:

```
tar -zxvf dazuko-2.3.9.tar.gz
cd dazuko-2.3.9/
./configure --without-dep
make
```

## test

### check environment:

```
lsmod | grep capability
capability                5896  0
commoncap                 8192  1 capability
```

note: since capability module is conflict with dazuko, need to remove capability first

```
sudo /sbin/modprobe -r capability
```

doing test install:

```
sudo make test
/sbin/modprobe commoncap
/sbin/insmod ./dazuko.ko
/sbin/rmmod dazuko
--> test successful :)
```

prepare loading script of dazuko by editing /etc/modprobe.d/dazuko as:

```
install dazuko /sbin/modprobe -r capability;\
/sbin/modprobe --ignore-install dazuko; \
/sbin/modprobe --ignore-install capability
```

add dazuko in modules file by appending at end of /etc/modules:

```
dazuko
```

reboot the box and after reboot run following command to verify:

```
lsmod | grep dazuko
dazuko                58596  0
commoncap             8192  2 capability,dazuko
```

## test

### run test example

```
cd dazuko-2.3.9/example_c
make
```

start the example to monitor any access in /home dir:

```
sudo ./example /home
```

test following operation:

```
sudo touch /home/test
sudo cat /home/test
sudo head -n 5 /home/user/dazuko-2.3.9/README
```

and the results are:

```
user@user-desktop: ~/dazuko-2.3.9/example_c
user@user-desktop:~/dazuko-2.3.9/example_c$ sudo ./example /home
DazukoIO version 2.3.9 (2.3.9.2)
registered with Dazuko successfully
Dazuko version 2.3.9 (2.3.9.2)
set access mask successfully
set scan path successfully
OPEN  uid:0 pid:5981 mode:33188 flags:1 file_uid:1000 file_gid:1000 file_mode:3
3188 file_device:0 file_size:0 file:/home/user/.sudo_as_admin_successful
OPEN  uid:0 pid:5981 mode:33188 flags:1 file_uid:0 file_gid:0 file_mode:33188 f
ile_device:0 file_size:0 file:/home/test

OPEN  uid:0 pid:5982 mode:33188 flags:1 file_uid:1000 file_gid:1000 file_mode:3
3188 file_device:0 file_size:0 file:/home/user/.sudo_as_admin_successful
OPEN  uid:0 pid:5982 mode:33188 flags:0 file_uid:0 file_gid:0 file_mode:33188 f
ile_device:0 file_size:0 file:/home/test

OPEN  uid:0 pid:5983 mode:33188 flags:1 file_uid:1000 file_gid:1000 file_mode:3
3188 file_device:0 file_size:0 file:/home/user/.sudo_as_admin_successful
OPEN  uid:0 pid:5983 mode:33188 flags:0 file_uid:1000 file_gid:1000 file_mode:3
3188 file_device:0 file_size:1382 file:/home/user/dazuko-2.3.9/README
█

user@user-desktop: ~
user@user-desktop:~$ sudo touch /home/test
user@user-desktop:~$ sudo cat /home/test
user@user-desktop:~$ sudo head -n 5 /home/user/dazuko-2.3.9/README
This directory contains the source code for the Dazuko driver.
Example programs to demonstrate the driver in C and Java are
available in the example_c and example_java sub-directories,
respectively.

user@user-desktop:~$ █
```

=====

## The call flow

TBD