dazuko: on access file system monitor

by eqmcc

dazuko: on access file system monitor	
Description	
Data structures	10,50
Test case	5
compile and install dazuko	5
test	7
The call flow	8
EQUUCCO HITCHIO	

Description

Regards, Frans.

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.

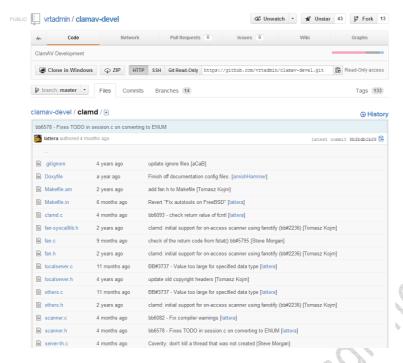
2. dazuko and DazukoFS is not used in clamav any more: http://lists.nongnu.org/archive/html/dazuko-help/2010-10/msg00002.html

Re: [Dazuko-help] It is dead?

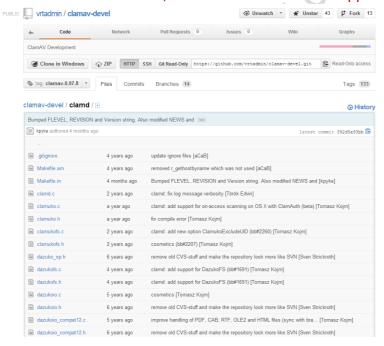
```
From: Frans de Boer
    Subject: Re: [Dazuko-help] It is dead?
        Date: Wed, 13 Oct 2010 20:22:05 +0200
User-agent: Mozilla/5.0 (X11; U; Linux x86_64; en-US; rv:1.9.1.12)
On 10/13/2010 10:41 AM, John Ogness wrote:
> Note: This email is being cross-posted to dazuko-devel since it
        contains 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.
```

Note:

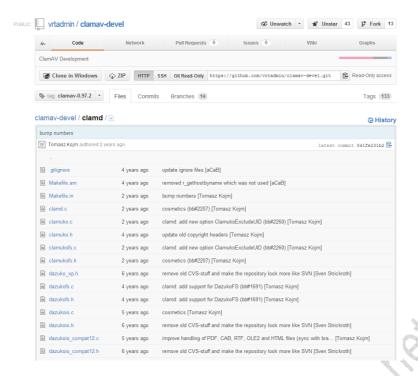
the support of dazuko/dazukoFS is lifted from version 0.98 using fanotify(fan.c):



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

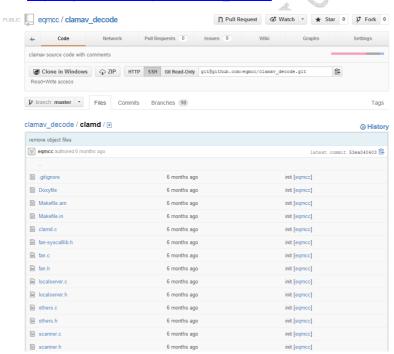


strange enough in clamav-dev repository in git hub, the version 0.97.2 is still supporting dazuko:



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

https://github.com/eqmcc/clamav decode



Data structures

TBD

Test case

TBD

compile and install dazuko

environment:

OS

Ubuntu 7.04(kernel verison: 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	Туре	File
(any of the following) RedirFS 0.8명 Linux 2.2.0 - 2.6.22 Linux/RSBAC명 FreeBSD 4 - 8명	kernel module CHANGELOG &	dazuko-2.3.9.tar.gzණ [MD5ණ] [GPGණ] 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-Oubuntu4)

check kernel version and complier

cat /proc/version

Linux version 2.6.20-15-generic (root@palmer) (gcc version 4.1.2 (Ubuntu 4.1.2-Oubuntu4)) #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:

Ismod | 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:

Ismod | 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

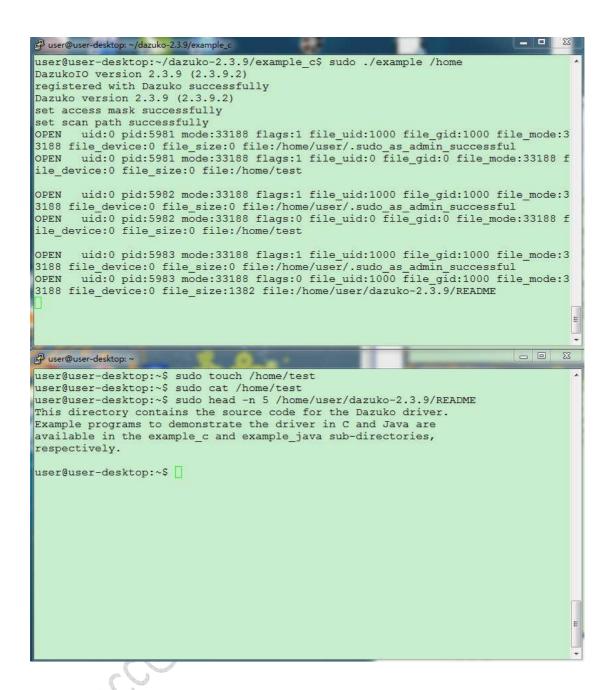
test following operation:

sudo touch /home/test

sudo cat /home/test

sudo head -n 5 /home/user/dazuko-2.3.9/README

and the results are:



The call flow

TBD