Into.the.Void.

Into The Void

28/08/2009

how to use encrypted loop files with a gpg passphrase in Debian

Fast howto (mostly a note for personal use) on what's needed on Debian to use an encrypted loop:

1. The necessary utilities (patched losetup)
```
# aptitude install loop-aes-utils
```
2. The necessary kernel-module
```
# aptitude install loop-aes-modules-2.6.30-1-686-bigmem
```
3. Create the keyfile (keep your computer as busy as possible while doing this to increase entropy)
```
# head -c 2925 /dev/urandom | uuencode -m - | head -n 66 | tail -n 65| gpg --symmetric -a >/path/to/keyfile.gpg
```
4. Loopfile creation (10Mb)
```
# dd if=/dev/urandom of=/my-encrypted-loop.aes bs=1k count=10000
```
5. Initialize loopfile
```
# losetup -K /path/to/keyfile.gpg -e AES256 /dev/loop5 /home/username/crypto-loop.img
```
6. Format loopfile
```
# mke2fs /dev/loop5
```
7. Delete loop device
```
# losetup -d /dev/loop5
```
8. Create mount point for loopfile
```
# mkdir /mnt/crypto-loop
```
9. Add entry to fstab

```
/home/username/crypto-loop.img /mnt/crypt-loop ext2
defaults,noauto,user,loop=/dev/loop7,encryption=AES256,gpgkey=/path/to/keyfile.gpg 0 0
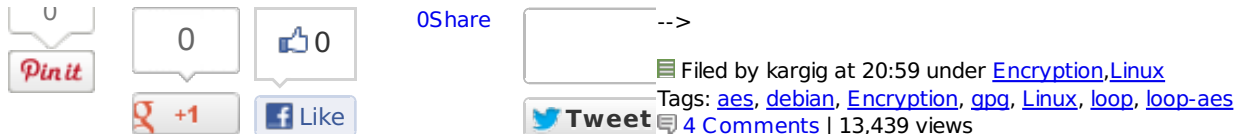```

10. Try mounting the loopfile as user
```
$ mount /mnt/crypto-loop
```
11. Check it's mounted properly
```
$ mount | grep -i aes
```

and use it!

P.S. Secure your keyfile.gpg, if it gets lost you won't _ever_ be able to decrypt what was inside crypto-loop.img!

## 4 Responses to "how to use encrypted loop files with a gpg passphrase in Debian"

1. argp
   August 29th, 2009 | 00:54
   Using 🌐 Debian IceWeasel 3.0.12 on 🌀 Debian GNU/Linux

   Nice post, thanks for the tip. However, I prefer encfs since it is a bit more platform independent.

2. how to use encrypted loop files with a gpg passphrase in Debian | Debian-News.net - Your one stop for news about Debian
   August 29th, 2009 | 20:30
   Using W WordPress 2.8.4

   [...] Fast howto (mostly a note for personal use) on what's needed on Debian to use an encrypted loop: More here [...]

3. leviathan
   September 3rd, 2009 | 00:11
   Using 🦊 Mozilla Firefox 3.0.13 on 🌀 Ubuntu Linux

   oraio file – perasa poly euxarista me TA mount points

4. Fuzzy Geek » Blog Archive » how to use encrypted loop files with a gpg passphrase in Debian
   September 30th, 2009 | 14:29

Using W WordPress 2.8.4

[...] i report a quick HOW-TO from http://www.void.gr , original post is  HERE [...]

# Leave a reply

name (required)

email (will not be shown) (required)

website

Submit Comment

Notify me of followup comments via e-mail

- 
- Search

## Links

- Home
- RSS

August 2009

| M | T | W | T | F | S | S |
|---|---|---|---|---|---|---|
|  |  |  |  |  | 1 | 2 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 |  |  |  |  |  |  |

« Jul                    Sep »

## Archives

- 2013
- 2012
- 2011
- 2010
- 2009
- 2008
- 2007
- 2006
- 2005
- 2004

- ## Recent Comments:

  - Jamen: I added this code to our local.cf, restarted Spamassassin, but about...
  - asghar: hello man could make a video tutorial of your nice article?
  - kargig: please send me an email so we can discuss details about the...

- **ercpe**: Thanks for this great plugin. Is there any chance to get support for...
- **kargig**: @Michael, yeah it's easy to throttle per sender, just add a...

## Most Viewed Posts:

- Some statistics on linux-greek-users mailing list and forum.hellug.gr - 68,897 views
- Openvpn – MULTI: bad source address from client – solution - 49,973 views
- There's a rootkit in the closet! - 48,767 views
- SSH Escape Characters - 34,416 views
- Greek adblock plus filter - 27,794 views
- Linux SSD partition alignment tips - 20,141 views
- rxvt-unicode 256 color support with vim - 18,776 views
- Cedega Warcraft III 1.20e nocd patch - 17,806 views
- kernel fun - 17,512 views
- Convert greek characters from latin1 mysql database fields to pure utf8 - 15,693 views

# Categories

- Encryption (19)
- General (175)
- Gentoo (37)
- Greek (31)
- Internet (94)
- IPv6 (15)
- Linux (233)
- MacOSX (8)
- maths (2)
- Networking (60)
- Privacy (35)
- Private (12)
- slogans (6)
- VoIP (5)

# Tag Cloud

adblock adblock plus ads antispam athens bash blacklist bug bugzilla debian DHCPv6 dns email firefox fluxbox fosscomm Gentoo gpg Greek grrbl https iceweasel Internet ipv6 Linux macbook MacOSX mysql Networking oneliner ossec perl plesk portage presentation Privacy script security slaac spam swiftfox tor vulnerability wordpress zsh

## Pages

- Contact
- Greek adblock plus filter
- GrRBL
- My dot files
- My PGP/GPG key
- Presentations/Articles

## Blogs

- modal echoes of the void
- $ dmesg_
- .: autoverse :.
- /home/idaru
- 0entropy
- About life, the universe and everything
- argp's blog
- Cyberpunk As a Commodity
- dimitris kalamaras
- Don't fear the penguin
- e-Προβατίνα
- Leonidas Tsampros
- nihil novo (nothing new)

- Reckoning
- vortex of false deceit
- Yet another open source blog ;)
- μα εγώ δεν ξέρω ρίμες

## Links

- Census Labs
- Ioannina Linux Users Group
- IPv6 material
- Planet Gentoo
- Planet Larry
- Planet Sysadmin

## Projects

- Greek AdblockPlus Filter
- HTTPS-Everywhere Greek Rules
- iloog
- Tormap

## Meta

- Log in

# Twitter Updates

- kargig: RT @grnetnoc: New rel of #FoD https://t.co/zRmCNnkmy4 adds fragment-type match.Could save you in a DNS-Amp #grnetnoc #bgpflowspec https: ...
- kargig: European regulators blast Google for continued EU privacy violations: http://t.co/gtGwCKoj0F
- kargig: Kinda sad that I have to remove the accounts of people/friends that we worked together and introduced me to the job :/
- kargig: @comzeradd "This video contains content from SME. It is restricted from playback on certain sites." ?!?!?!?!?!?!?!?!?
- kargig: RT @bm_: best bootstrap theme ever, though have to say the progress bars are a bit sloppy http://t.co/aciyIvXJ6f

follow me on Twitter

# Visits

9 online / 2055909 total

Using a modified Gentle Calm theme.

W o r d P r e s s took 0.604 seconds to generate this XHTML page.