Πως να δημιουργήσετε ένα κρυπτογραφημένο περιβάλλον σε GNU/Linux με πυρήνα 2.6 με το dm_crypt

1.0) Εισαγωγή.

1.1) Τι είναι το dm_crypt?

Το "device mapper" (dm) είναι το νέο σύστημα δημιουργίας εικονικών διαστρώσεων (virtual layer) συσκευών αποθήκευσης (block devices) για τον πυρήνα 2.6 . Το dm "κάθεται" πάνω σε συσκευές που το σύστημα αναγνωρίζει ως "πραγματικές", όπως σκληρούς δίσκους και κατατμήσεις (partitions). Οι χρήσεις του είναι πολλαπλές, μπορεί να χρησιμοποιηθεί για να συνδέσει εικονικά δύο ή παραπάνω συσκευές, να πάρει μια "εικόνα" (snapshot) αυτόματα κτλ. Γνωστά προγράμματα που χρησιμοποιούν αυτό το εικονικό σύστημα διαχείρισης συσκευών είναι και τα "LVM2" και "EVMS".

Ανάμεσα στις χρήσεις του είναι και η κρυπτογράφηση. Το "device mapper" επιτυγχάνει την κρυπτογράφηση διαμέσου του "dm_crypt", ενός αρθρώματος (module) το οποίο δημιουργεί ένα "διαφανές"[1] κρυπτογραφημένο περιβάλλον παρέχοντας στον χρήστη την απαιτούμενη άσφάλεια χωρίς να του στερεί την άνεση.

Το "dm_crypt" είναι διάδοχος του "crypto-loop-device", έχει πιο καθαρογραμμένο κώδικα και είναι πιο ελαστικό από τον πρόγονο του. Μπορείτε να βρείτε περισσότερες πληροφορίες για το "dm_crypt" στον δικτυακό τόπο: http://www.saout.de/misc/dm-crypt/

1.2) Δυο λόγια για την κρυπτογραφία.

Η κρυπτογραφία είναι πολύ μεγάλο και πολύ περίπλοκο θέμα για τους απλούς χρήστες. Παρόλ' αυτά, αφού την χρησιμοποιούμε καθημερινά καλό είναι να γνωρίζουμε κάποια βασικά πράγματα γι αυτήν.

Αρχικά η κρυπτογραφία ήταν αποκλειστικό προνόμιο του στρατού και τον διάφορων κυβερνητικών υπηρεσιών για ευνόητους λόγους. Πολλοί θα γνωρίζετε τον μύθο του αλγόριθμου "enigma"[2]. Λέγετε ότι ο "enigma" άλλαξε την πορεία του δευτέρου παγκοσμίου πολέμου σε βάρος των Γερμανών κι έθεσε την βάση για την σημερινή μορφή της κρυπτογραφίας.

Σήμερα έχουμε στην διάθεση μας αλγόριθμους παντοδύναμους που μπορούν να καλύψουν το μεγαλύτερο μέρος των αναγκών μας όπως οι AES, Serpent, Blowfish και IDEA. Ένας αλγόριθμος κρυπτογράφησης θεωρείτε ασφαλής όταν μείνει ελεύθερος για μεγάλο χρονικό διάστημα χωρίς να καταφέρει κάποιος να τον αποκρυπτογραφήσει εξ ολοκλήρου ή μερικός. Η κρυπτογραφία δεν χωρίζεται μόνο σε αλγόριθμους αλλά και σε τρόπους εφαρμογής[3]. Ο τρόπος εφαρμογής είναι συχνά το αδύνατο σημείο ενός προγράμματος που χρησιμοποιεί την κρυπτογραφία, αυτό είναι καλό να το έχουμε υπόψιν όταν πρέπει να επιλέξουμε ανάμεσα σε προγράμματα που κάνουνε χρήση της κρυπτογραφίας.

2.0) Εγκατάσταση.

2.1) Εγκατάσταση του cryptsetup, πυρήνας και εργαλεία συστήματος.

Τι χρειαζόμαστε?

1. Ένα πυρήνα ανώτερο του 2.6.4 [4]
2. Να εγκαταστήσουμε το cryptsetup

2.1-α) Διαμόρφωση πυρήνα

Τώρα πρέπει να διαμορφώσουμε τον πυρήνα, οι απαιτούμενες επιλογές είναι οι εξής:

Code maturity level options --->
<*> Prompt for development and/or incomplete code/drivers

Device Drivers ---> Generic Driver Options --->
<M> Hotplug firmware loading support

Device Drivers ---> Multi-device support (RAID and LVM) --->
<M> Device mapper support
<M> Crypt target support

Cryptographic options --->
<M> AES cipher algorithms
<M> Serpent cipher algorithm

ΠΡΟΣΟΧΗ: *επιλέξτε τον αλγόριθμο της αρεσκείας σας, τα παραδείγματα είναι με τον AES (Advanced Encryption Standard) αφού είναι πιο διαδεδομένος αλγόριθμος απ' όλους. Άλλοι αλγόριθμοι που προτείνονται είναι οι Blowfish, serpent.*
*Ο υποφαινόμενος υποθέτει ότι οι χρήστες του πυρήνα 2.6.5 και άνω έχουνε **udev**. Αν έχετε devfs θα πρέπει να δώσετε f**ull path** κι όχι απλώς /dev/hdX ή /dev/sdX, να το θυμάστε γιατί δεν θα αναφερθεί αργότερα εφόσον το devfs θεωρείτε ξεπερασμένο από τους kernel developers.*

2.1-β) Εγκατάσταση cryptsetup

Το πρόγραμμα με το οποίο θα χειριζόμαστε το κρυπτογραφημένο περιβάλλον είναι το cryptsetup. Για να το εγκαταστήσουμε όμως θα χρειαστούμε την βιβλιοθήκη dmsetup και το πακέτο hashalot.[5] Μπορείτε να βρείτε τα πακέτα στο διαδύκτιο ή να κατεβάσετε με το σύστημα διαχείρισης πακέτων της διανομής σας. Η debian και η gentoo χειρίζονται αυτόματα τις απαιτήσεις του προγράμματος.

[Στο τέλος του κειμένου θα βρείτε περισσότερες πληροφορίες σχετικά με τα πακέτα που υπάρχουν για την διανομή σας.]

2.2) Δημιουργία κρυπτογραφημένου περιβάλλοντος

Αρχικά ελέγχουμε εάν το device mapper λειτουργεί σωστά:

```
root # ls -l /dev/mapper/
total 0
crw-rw----  1 root root 10, 63 Jun 28 01:41 control
```

Εάν κάτι πάει στραβά ελέγξτε με το lsmod τα φορτωμένα αρθρώματα κι αν δεν είναι στην λίστα, απλώς φορτώστε το:

```
root # modprobe dm_crypt
```

Έπειτα φορτώστε τον αλγόριθμο κρυπτογράφησης που επιλέξατε:

```
root # modprobe aes
root # cat /proc/crypto
name         : aes
module       : aes
type         : cipher
blocksize    : 16
min keysize  : 16
max keysize  : 32
```

Τώρα πλέον ελέγχουμε το dmsetup για να δούμε αν όλα είναι έτοιμα:

```
root # dmsetup targets
crypt           v1.0.0
striped         v1.0.1
linear          v1.0.1
error           v1.0.1
```

Τώρα πρέπει να κάνουμε την επιλογή κλειδιού. Οι επιλογές που θα ήθελα να προτείνω είναι 2:

1. Κωδικός ασφαλείας.
2. Δημιουργούμε ένα κλειδί σε εξωτερική συσκευή αποθήκευσης.

Οι δύο περιπτώσεις έχουνε πλεονεκτήματα και μειονεκτήματα. Ανάλογα με την περίπτωση και την χρήση που θα κάνουμε. Επειδή εγώ κάνω εκτεταμένη χρήση για το σύστημα αρχείων μου, δεν θέλω σε κάθε επανεκκίνηση να βάζω ένα αδύναμο κωδικό γι' αυτό διάλεξα την δεύτερη περίπτωση.

1) Κωδικός ασφαλείας

Πρέπει να έχουμε έτοιμη την κατάτμηση την οποίο θέλουμε να κρυπτογραφήσουμε. Καλό είναι να κάνετε επανεκκίνηση μετά από κάθε αλλαγή στον πίνακα κατατμήσεων του υπολογιστή (partition table). Δημιουργούμε το σύστημα αρχείων με κωδικό:

```
root # cryptsetup -y -c aes create secret /dev/hdaX
```

Με αυτήν την εντολή δημιουργήσαμε μια εικονική συσκευή, η οποία λέγετε "secret", είναι στον κατάλογο /dev/mapper/ κι είναι συνδεδεμένη με την συσκευή /dev/hdaX. Η παράμετρος "-c" καθορίζει τον αλγόριθμο κρυπτογράφησης.

Το "hdaX" πρέπει να το αντικαταστήσετε με την κατάτμηση της επιλογής σας, ενώ η παράμετρος "-y" θα ζητήσει επαλήθευση του κωδικού. Η παράμετρος "create" δηλώνει στο cryptsetup την ενέργεια που θα πρέπει να εκτελέση. Το cryptesetup έχει κι άλλες δυνατότητες, μπορείτε να τις ελέγξετε με την παράμετρο –help ως εξής:

```
root # cryptsetup --help
Usage: cryptsetup [OPTION...] <action> <name> [<device>]
  -v, --verbose             Shows more detailed error messages
  -c, --cipher=STRING       The cipher used to encrypt the disk (see
                            /proc/crypto) (default: "aes")
  -h, --hash=STRING         The hash used to create the encryption key from
                            the passphrase (default: "ripemd160")
  -y, --verify-passphrase   Verifies the passphrase by asking for it twice
  -d, --key-file=STRING     Read the key from a file (can be /dev/random)
  -s, --key-size=BITS       The size of the encryption key (default: 256)
  -b, --size=SECTORS        The size of the device
  -o, --offset=SECTORS      The start offset in the backend device
  -p, --skip=SECTORS        How many sectors of the encrypted data to skip
                            at the beginning

Help options:
  -?, --help                Show this help message
  --usage                   Show this help message
```

<action> is one of:
create - create device
remove - remove device
reload - modify active device
resize - resize active device
status - show device status
<name> is the device to create under /dev/mapper
<device> is the encrypted device

2) Δημιουργία κλειδιού με εξωτερική συσκευή αποθήκευσης.

Η συσκευή αποθήκευσης μπορεί να είναι οποιαδήποτε συσκευή είναι συνδεδεμένη με τον υπολογιστή μας ο οποίος είναι σε θέση να διαβάσει ή να γράψει δεδομένα σε αυτήν, όπως ένας εξωτερικός σκληρός δίσκος USB, ένα cdrom ή μια δισκέτα. Το παράδειγμα θα γίνει με μια δισκέτα.

ΠΡΟΣΟΧΗ: *Οι δισκέτες γενικά χαλάνε πολύ εύκολα και πολύ συχνά. Σιγουρευτείτε ότι η δισκέτα δουλεύει σωστά. Κάντε οπωσδήποτε fdformat και mkfs.ext2. Μπορείτε να αντιγράψετε το κλειδί σε κάποιο ασφαλές cdrom ή άλλη συσκευή αποθήκευσης η οποίο θα φυλάσσετε μακριά από τον υπολογιστή.*

Δημιουργούμε το κλειδί το οποίο θα αντιγράψουμε στην δισκέτα:

root # dd if=/dev/urandom of=key bs=12k count=100

Στο παράδειγμα κάναμε ένα κλειδί μεγέθους 1.2 MB. Μπορείτε να το κάνετε μικρότερο η μεγαλύτερο. Το κάνουμε copy στην δισκέτα που έχουμε ετοιμάσει και δημιουργούμε το κρυπτογραφημένο περιβάλλον:

root # cp key /mnt/floppy/
root # cryptsetup -c aes -d /mnt/floppy/key create secret /dev/hdaX

Ελέγχουμε αν όλα πήγανε καλά:

root # dmsetup ls
secret (253, 0)

Εάν όλα γίνανε επιτυχώς τότε, έχετε δημιουργήσει μια εικονική διάστρωση (virtual layer) ανάμεσα στην κατάτμηση και την συσκευή /dev/mapper/secret *[ή όπως την ονόμασε ο χρήστης]*.
Έπειτα δημιουργούμε το σύστημα αρχείων της συσκευής. Προσοχή το σύστημα αρχείων το δημιουργούμε επάνω στο /dev/mapper/secret:

root # mkfs.xfs /dev/mapper/secret

Φυσικά μπορείτε να διαλέξετε τον τύπο κατάτμησης. Εγώ επέλεξα το xfs γιατί είναι πιο γρήγορο στην διαχείριση μεγάλων αρχείων. Αν όλα έχουνε πάει καλά μπορούμε να προσαρτήσουμε (mount) την κατάτμηση:

root # mkdir /mnt/secret/
root # mount -t xfs /dev/mapper/secret /mnt/secret -v

Ελέγξτε με τις εντολές "mount" και "df" αν όλα είναι εντάξει. Αν όλα είναι εντάξει, μπορείτε να μεταφέρετε όλα τα αρχεία σας στο κρυπτογραφημένο περιβάλλον, από εδώ και πέρα το dm_crypt τα κρυπτογραφεί αυτόματα.
Θέλει πολύ **προσοχή** ο τρόπος με τον οποίο κάνουμε την απο-προσάρτηση (unmount) της κρυπτογραφημένης κατάτμησης:

root # umount /mnt/secret -v
root # cryptsetup remove secret

ΠΡΟΣΟΧΗ: E*άν δεν γίνει μετακίνηση της κατάτμησης με το cryptsetup, θα μπορεί ο καθένας με δικαιώματα διαχειριστή να προσάρτηση την κατάτμηση χωρίς να χρειάζεται ο κωδικός ή το κλειδί!!!*

Ελέγχουμε ότι όλα πήγανε καλά στην μετακίνηση:

root # dmsetup ls

εάν έχει γίνει επιτυχημένα η απο-προσάρτηση και η μετακίνηση δεν θα σας δείξει **τίποτε** το dmsetup[6]. Δεν θα βγάλει μήνυμα λάθους. Μπορείτε να πάρετε κι άλλες πληροφορίες πληκτρολογώντας:

root # dmsetup info <secret>

3.0) Τελικά σχόλια και παραπομπές.

3.1) Scripts για αυτόματη διαχείριση.

Τελειώνουμε με δύο πολύ απλά προγραμματάκια για να κάνετε αυτόματα τις προσαρτήσεις και απο-προσαρτήσεις και για τις δύο περιπτώσεις:

1) Κωδικό ασφαλείας
crypt-up

```
#!/bin/bash

/usr/sbin/cryptsetup -c aes create secret /dev/hdaX -v
mount /dev/mapper/secret /mnt/secret -v
```

crypt-down

```
#!/bin/bash
umount /mnt/secret -v
/usr/sbin/cryptsetup remove secret -v
```

2) Διαχείριση κλειδιού με εξωτερική συσκευή αποθήκευσης.
crypt-up

```
#!/bin/bash
mount -t ext2 /dev/fd0 /mnt/floppy -v
/usr/sbin/cryptsetup -c aes -d /mnt/floppy/key create secret /dev/hdaX -v
mount /dev/mapper/secret /mnt/secret -v
umount /dev/fd0 -v
```

crypt-down

```
#!/bin/bash
umount /mnt/secret -v
/usr/sbin/cryptsetup remove secret -v
```

Μπορείτε να τα κάνετε chmod a-rwx,u+xr και να τα βάλετε στο $PATH του root για μεγαλύτερη άνεση.

3.2) Διάφορα σχόλια και συμβουλές.

Το κρυπτογραφημένο περιβάλλον που δημιουργήσετε είναι μια προχωρημένη μορφή ασφαλείας. Υπάρχουνε κάποια προβλήματα που μπορεί να συναντήσετε. Η κρυπτογράφηση λόγο της φύσης της είναι επίπονη για τον υπολογιστή. Υπολογιστές με μικρό επεξεργαστή, παλιότερης τεχνολογίας ίσως ζοριστούνε πολύ εάν μεταφέρετε μεγάλα αρχεία στο κρυπτογραφημένο περιβάλλον. Καλό είναι να έχετε έναν υπολογιστή στα 600 Mhz τουλάχιστον εάν θέλετε να δημιουργήσετε ένα διακοσμητή κρυπτογραφημένων αρχείων για να διαχειρίζεται μεγάλα αρχεία με άνεση.

Εάν δεν έχετε κάποια κατάτμηση ελεύθερη μπορείτε πάντοτε να δημιουργήσετε ένα με την εντολή "dd".

Εάν θέλετε μια κρυπτογραφημένη κατάτμηση τύπου "swap" μπορείτε να δημιουργήσετε ένα απλό "script" σαν αυτό:

```
!#/bin/bash
cryptsetup -c serpent -d /dev/urandom create   enc-swap  /dev/hdb1
mkswap /dev/mapper/enc-swap
swapon /dev/mapper/enc-swap
```

το οποίο θα εκτελείτε σε κάθε εκκίνηση.

Εάν θέλετε να κρυπτογραφήσετε μικρά αρχεία η οτιδήποτε άλλο, ρίξτε μια ματιά στο "mcrypt". Κατά την ταπεινή μου άποψη είναι ό,τι καλύτερο, ενώ υπάρχει και σαν πακέτο για τις περισσότερες διανομές, μπορείτε να το βρείτε εδώ http://mcrypt.hellug.gr

3.3) Παραπομπές

[1] Διαφανής αποκαλείται η εργασία που δεν γίνεται αντιληπτή από τον χρήστη. Αφού εγκατασταθεί το dm_crypt ο χρήστης δεν θα πρέπει να ασχοληθεί ξανά με την κρυπτογράφηση και την αποκρυπτογράφηση των δεδομένων, αφού θα την χειρίζεται εξ ολοκλήρου το dm_crypt.

[2] ENIGMA and the II WW: http://www.codesandciphers.org.uk/enigma/index.htm

[3] http://ftp.magicsoftware.com/www/help/iBOLT/Encryption_-_Supported_Encryption_Methods_and_Modes.htm

[4] Ο πυρήνας 2.6.4 έχει μια τρύπα ασφαλείας στην εφαρμογή του dm_crypt η οποία διορθώθηκε στην επόμενη έκδοση του πυρήνα.

[5] Εγκατάσταση cryptsetup και dependencies:
Πυρήνας GNU/Linux: http://www.kernel.org
Cryptsetup και dependencies:

Fedora Linux: υπάρχουν τα rpm's
Mandrake Linux: υπάρχουν τα rpm's
Gentoo GNU/Linux: http://bugs.gentoo.org/show_bug.cgi?id=54663
Debian GNU/Linux: apt-get install dmsetup
apt-get install hashalot

[6] Δοκιμάστε με το flag -v ίσως πάρετε μύνημα :)

[*] Cryptsetup πηγαίος κώδικας: http://www.saout.de/misc/dm-crypt

---

Ευχαριστίες: dtb, djart, tachyon, r00thell, hellug, Open Source, Linus Torvalds.
Οποιοδήποτε feedback είναι ευπρόσδεκτο: blade@teilam.gr
Mario (BladE^) Saturno