Cryptoloop

Thomas Jampen
<jampen@cryptography.ch>

Outline

- Introduction & history
- Kernel configuration
- losetup and mount
- Encrypted home directory
- Encrypted swap partition
- Security Issues
- Outlook

Introduction

- Filesystems (fs) stored within a single file can be mounted over a loopback device

```
mount -o loop -t iso9660 some.iso /mnt
```

- Such fs can be transparently encrypted using an extension of the loop driver called

cryptoloop

History I

- International crypto patch
  - Since kernel 2.2.9
  - http://www.kerneli.org
  - Includes cryptographic api (ciphers and message digests) and cryptoloop driver
  - Patches needed for util-linux (losetup and mount)

History II

- Cryptographic API included
  - Since kernel 2.4.22
  - Patch needed for cryptoloop support
  - http://www.kernel.org/pub/linux/kernel/crypto/v2.4/testing/
- Cryptoloop support included
  - Since kernel 2.6

Kernel I

- Patch the kernel (>= 2.4.22)
  - http://www.kernel.org/pub/linux/kernel/crypto/v2.4/testing/cryptoloop-jari-2.4.22.0
  - cd /usr/src/linux
  - patch -p1 < /path/to/patch-cryptoloop-jari-2.4.22.0
- No patch needed for kernel 2.6.x
- Patch util-linux (if necessary)

Kernel II

- Configure the kernel
  - under Block Devices
  - enable Loopback device support
  - enable Cryptoloop support

  - under Cryptographic options
  - enable cipher(s) (e.g. twofish cipher)
- Compile the kernel
- Load modules (if necessary)

Creating Encrypted FS

```
• dd if=/dev/urandom of=~/data bs=1M count=100
• losetup -e twofish -k 256 /dev/loop0 ~/data   *
• mkfs.ext2 /dev/loop0
• mkdir ~/crypto
• mount -t ext2 /dev/loop0 ~/crypto             *

• umount ~/crypto                               *
• losetup -d /dev/loop0                         *
```

- Only repeat indicated (*) steps later on

Using /etc/fstab

- Line to add to /etc/fstab

```
/home/foo/data    /home/foo/crypto/    ext2 \
defaults,noauto,user,exec,loop=/dev/loop0, \
encryption=twofish,keybits=256    0    2
```

- Mount encrypted fs with

```
foo@compi:~$ mount crypto
Password:
foo@compi:~$
```

- A normal user can mount the fs if he owns the mountpoint

Encrypted /home/foo

- /home/foo/data can be mounted over /home/foo!
- Either add mount command to ~/.bash_profile
  - Console login only
  - X login can't ask for passphrase
- or use pam-mount
  - Can mount SMB/NCP shares and loopback enc fs
  - No need to enter two passwords
  - No need for entry in /etc/fstab

Configuring pam-mount

- Modify configuration file /etc/security/pam_mount.conf
- Add a line for each volume

```
volume foo local - /home/foo/data /home/foo \
loop=/dev/loop0,encryption=twofish,keybits= \
256,user,exec aes-256-ecb /home/foo/key
```

- fsckloop defines the loop device to be automatically used in order to fsck each fs before mounting it

Configuring PAM

- Add the following lines to the desired service file(s) (e.g. /etc/pam.d/login)

```
auth    optional  pam_mount.so  use_first_pass
session optional  pam_mount.so
```

- Debian automatically installs a file called common-pammount. Include this file with

```
@include common-pammount
```

Creating Encrypted Home FS

-
  ```
  dd if=/dev/urandom of=/home/foo/data bs=1M \
  count=<size in MB>
  ```

-
  ```
  dd if=/dev/urandom bs=1c count=32 | \
  openssl enc -aes-256-ecb > /home/foo/key
  (count=<key size / 8>)
  ```

-
  ```
  openssl enc -d -aes-256-ecb -in \
  /home/foo/key | losetup e twofish -k 256 \
  -p0 /dev/loop0 /home/foo/data                  *
  ```

-
  ```
  mkfs.ext2 /dev/loop0                           *
  ```

-
  ```
  losetup -d /dev/loop0                          *
  ```

- Steps marked with (*) require root privileges

Encrypted Swap Partition

- Cryptoloop can be used to encrypt the swap partition
- Init script chooses a random pwd
- Install init script
  - Debian
    - `update-rc.d encrypted-swap start 34 S . \`
      `start 41 0 6 .`
  - Other distributions
    - add symlinks (start early, stop late)
  - Comment out swap entry in /etc/fstab!

Enc Swap Init Script I

```
#!/bin/sh

SWAP=/dev/hda6          # swap partition or file
LOOP=/dev/loop1         # the loop device to use
ALG=twofish             # cipher algorithm
KEY=256                 # key size

case "$1" in
  start)
    echo "Initializing encrypted swap space... "
    # modprobe cryptoloop (cipher-)$ALG # if needed
    /bin/dd if=/dev/urandom bs=1c count=32 \
    2> /dev/null | /usr/bin/mimencode | \
    /sbin/losetup -p0 -e $ALG -k $KEY $LOOP $SWAP
    /sbin/mkswap $LOOP >/dev/null 2>&1
    /sbin/swapon $LOOP
    echo "done."
    ;;
```

Enc Swap Init Script II

```
  stop)
    echo -n "Umounting encrypted swap space... "
    /sbin/swapoff $LOOP
    /sbin/losetup -d $LOOP
    echo "done."
    ;;
  status)
    /bin/cat /proc/swaps
    ;;
  restart)
    $0 stop
    $0 start
    ;;
  *)
    echo "Usage: $0 {start|stop|restart|status}"
    exit 1
esac
```

Security Issues

- Cryptoloop is vulnerable to optimized dictionary attack
  - Most (if not all) fs have known plaintext (e.g. byte offset 0x600 – 0x60F: bits are 0)

    -
      ```
      dd if=/dev/hdaX bs=16 skip=96 count=1 \
      2> /dev/null | od -An -tx1 -
      ```
  - Most distributions use unsalted and uniterated passphrases which means a direct connection between passphrase and ciphertext
  - IV is predictible (related to block number)
  - Ciphertexts can be precomputed (dictionary)

General Remarks

- Journaling filesystems
  - Don't use journaling filesystems on file backed loop devices
  - Device backed loop devices can use journaling filesystems (disable write cache)
- Don't use suspend-to-disk!

Alternatives I

- loop-aes (Jari Ruusu)
  - http://www.sf.net/projects/loop-aes
  - Uses loopback device
  - No need to patch the kernel (2.2, 2.4 and 2.6)
  - Disable Loopback device support in kernel!
  - Corrects some security issues
  - Limited to AES cipher
  - Needs patched util-linux package

Alternatives II

- dm-crypt (Christophe Saout)
  - http://www.saout.de/misc/dm-crypt
  - Does NOT use loopback device
  - Included in kernel since 2.6.4
  - Can be found under Multi-device support
  - Cryptoloop maintainer (Fruhwirth Clemens):
    - It does not suffer from loop.c bugs (There are a lot, no maintainer)
    - dm-crypt does not depend on special user space tool (util-linux)
    - dm-crypt uses mempool, which makes it rock stable compared to cryptoloop