Encrypting Swap investigation report

April 29, 2015

1 Introduction

There are two schemes of encrypting swap partition:

A: Encrypt the partition underlying the file system, which works at the block level. This can be done by using some libs/utilities such as blivet. Through this we can protect sensitive data on the disks which have been swapped from the memory. Once a disk is encrypted in this method, it will require the user to input the passphrase when system boots to decrypt the disk.

B: Encrypt the partition by kernel during running time. In this scheme, the cycle of encryption begins when system boots and ends when system shuts down. This can prevent some user processes to access sensitive data on swap partition which they have no authority. In this method we can set a random passphrase generated from /dev/urandom.

Scheme B is which we are seeking to implement and the following is a verified solution for scheme B.

Section 4 gives a solution for scheme A.

2 Example of the solution for B:

Steps:

1. Have a partition prepared.
2. Configure /etc/fstab.
   /dev/mapper/**abc** swap swap defaults 0 0
3. Configure /etc/crypttab.
   abc **/dev/sdb2** /dev/urandom swap
4. Reboots.

Explanation:

There is no extra requirement to the partition, meaning that it does not even need to be set as 'swap' when it is created. So this solution has nothing to do with blivet. Any existing partition can be used here, but once it is configured as above, any data on the partition will be destroyed when system reboots.

In these two configure files, you change only two strings: "abc" and "/dev/sdb2".

1. Replace "abc" with any regular string, just making sure the consistency between the two files.

2. Replace the "/dev/sdb2" with the path of the partition which you want to use as an encrypted swap.

3 How to verify the result?

- **Check if it is used as a swap**

  Use 'swapon -s' to list all active swaps, the output is as follows:

  /dev/dm-2 partition 102396 0 -1

  Use 'ls -l /dev/mapper' to locate the path of the swap, as:

  lrwxrwxrwx. 1 root root 7 Apr 22 02:10 abc -> ../dm-2

  From this we can confirm that /dev/mapper/abc (/dev/dm-2) is now a swap.

- **Check if it is encrypted**

  Use 'dmsetup ls –target=crypt' to list all encrypted devices, as:

  abc (253, 2)

  From this we can confirm that 'abc' is an encrypted device.

4 Solution for scheme A

```
1 import blivet
2
```

```
3  b=blivet.Blivet()
4  b.reset()
5
6  sdd=b.devicetree.getDeviceByName(''sdd'')
7  disks=[sdd]
8
9  for i in disks:
10   b.recursiveRemove(i)
11
12 for i in disks:
13   b.initializeDisk(i)
14
15 # Create a partition for use
16 factory = blivet.devicefactory.PartitionFactory(
17           b, 350, disks, fstype=''swap'',
18           encrypted = True, name=''test'' )
19 factory.configure()
20
21 # Set passphrase and map name for encrypted partitions
22 for device in b.devices:
23     if device.format.type ==  ''luks'' and
24         not device.format.exists:
25         if not device.format.hasKey:
26             device.format.passphrase = ''123456''
27             device.format.mapName = ''encrypt''
28
29 b.doIt()
```

5 Reference

Running 'man 5 crypttab' on linux is a good reference.