Enabling Encrypted Swap

When available memory drops below a certain point, the Linux kernel will swap the contents of memory pages to swap space.

This content may include sensitive information such as passwords, usernames, PINS, banking or other identity information. This data is usually in plain text and so can be read without effort. Encrypting the system swap space protects its contents against unauthorized access and attack should access to the hard drive be compromised or physically removed.

Setting up Encrypted Swap

The following discussion will use several drive and partition designations. Be sure when implementing the procedures to adjust these to suit your own system.

The steps that follow can be used when initially setting up a system, or after a system is already running. If the latter, the first step required to encrypt the swap partition is to temporarily turn off swap. Close all unnecessary applications to free used memory and thereby discontinue the use of the swap space. While many applications can be configured to not use swap, this does not apply to the kernel. If the swap space is still being used, you will be unable to turn off swap.

Though not necessary, perhaps the simplest approach is to boot the system into single user mode. This results in minimal services running and a single root shell.

Swap can then be turned off using the following command:

```
# swapoff -a
```

To ensure a completely clean and sterile swap space, you must overwrite the previously used swap partition with random data. This will help prevent the recovery of any data written to swap before the encryption process. There are several ways to do this.

The following steps will destroy the current contents on the specified device/partition!

Perhaps the easiest is using the shred command which overwrites the specified file or device with random data:

```
# shred -v /dev/sdaX
```

Alternatively, overwriting the space with random data from either /dev/random or /dev/urandom:

```
# dd if=/dev/random of=/dev/sdaX bs=512
```

or

```
# dd if=/dev/urandom of=/dev/sdaX bs=512
```

Using /dev/urandom is not quite as secure, however it is significantly faster than using /dev/random.

The next step is to create a file, if it doesn't already exist, named crypttab in /etc. The specifics for crypttab can be found in the man page.

A crypttab entry as follows creates an encrypted block device named swap at /dev/mapper using the partition /dev/sdX as the base block device and /dev/random as the encryption password using AES encryption and variable initialization vectors.

```
swap /dev/sdaX /dev/random swap,cipher=aes-xts-essiv:sha256
```

You then need to edit /etc/fstab to point to the encrypted block device, /dev/mapper/swap as opposed to /dev/sdaX.

For example a current entry of:

```
/dev/sdaX swap swap defaults 0 0
```

becomes:

```
/dev/mapper/swap swap swap defaults 0 0
```

Activating Encrypted Swap

You can now enable encrypted swap either by rebooting the system or by issuing the following commands at the console prompt.

```
# cryptsetup -d /dev/random create swap /dev/sdaX
```

```
# mkswap /dev/mapper/swap
```

```
# swapon -a
```

For detailed information on specific commands please see the individual manual (man) pages.

Sources

Original source: Slackware Encrypted Swap Originally written by W. Dean Milner

howtos, security, encryption, swap