Agence Nationale
de la Sécurité des
Systèmes d'Information

Mémo : Effacement manuel d'un poste bureautique Clip

Mots-clés : effacement, poste

Table des matières

~~DIFFUSION LIMITÉE~~

1 Pré-requis

Liste des pré-requis :

- Le poste bureautique portable CLIP à effacer ;
- Installeur CLIP ;

2 Préambule

Il faut démarrer le poste sur le support d'installation de CLIP, choisir de démarrer un environnement graphique, puis ouvrir un terminal une fois que l'environnement graphique est démarré.

Dans ce terminal il convient de distinguer, dans le répertoire « /dev », le « device » d'installation de celui du disque sur lequel CLIP est installé. Si le support d'installation de CLIP est un dvd ou cdrom la question ne se pose pas. Par contre si il s'agit d'une clé USB d'installation de CLIP, elle apparaîtra comme un disque. Le « device » de la clé sera alors celui pour lequel le « LABEL » affiché par « blkid » est « clip-livecd ».

L'effacement du disque, qu'il s'agisse d'un disque magnétique ou d'un ssd, comprend trois phases successives réalisées dans l'ordre suivant :

- la suppression des Host Protected Area, si il en existe,
- l'effacement du contenu des secteurs du disque,
- l'effacement de sécurité du disque.

3 Suppression des Host Protected Area

Le HPA (Host Protected Area) permet de limiter la taille visible d'un disque dur, il est surtout utilisé pour stocker des partitions de récupération.

A priori un disque sur lequel a été installé CLIP ne contient pas de HPA mais il peut être utile de le tester grâce à la commande « hdparm –N /dev/sdX », « /dev/sdX » correspondant au disque sur lequel CLIP est installé. Par exemple :

Sans HPA :

```
# hdparm -N /dev/sdX
```

retourne

```
# max sectors = 156250000/156250000, HPA is disabled
```

Avec HPA :

```
# hdparm -N /dev/sdX
```

retourne

```
# max sectors = 156050000/156250000, HPA is enabled
```

Désactivation :

```
# hdparm -Np156250000 /dev/sdX
```

retourne

```
# setting max visible sectors to 156250000 (permanent) max sectors =
    156250000/156250000, HPA is disabled
```

4 Effacement du contenu des secteurs du disque dur

Il y a deux manières de procéder à l'effacement du contenu des secteurs du disque dur :

- en demandant au firmware du disque d'effacer l'ensemble des secteurs du disque à l'aide de la commande « blkdiscard »,
- en demandant au pilote du système d'exploitation de réécrire (surcharge) diverses valeurs sur l'ensemble du disque dur, à l'aide des commandes « shred » et « dd ».

La commande « blkdiscard » n'est pas supportée par tous les modèles de disque, toutefois on la préférera aux commandes de réécriture quand elle l'est. Pour savoir si « blkdiscard » est supportée par le disque il suffit de tester la procédure d'effacement l'utilisant. Cette procédure échouera immédiatement si blkdiscard n'est pas supportée.

Si « blkdiscard » n'est pas supportée on pratiquera l'effacement par surcharge.

4.1 Effacement par blkdiscard

L'effacement sécurisé de l'ensemble du disque « /dev/sdX » est obtenu par la commande :

```
# blkdiscard -s /dev/sdX
```

4.2 Effacement par surcharge

L'effacement par surcharge comprend d'abord un appel à « shred » :

```
# shred -v /dev/sdX
```

Puis une passe de mise à zéro :

```
# dd if=/dev/zero of=/dev/sdX  bs=4k  count=250000
```

avec l'argument « count » adapté à la taille du disque à effacer.

5 Effacement de sécurité

Il faut commencer par s'assurer que le disque supporte la commande ATA Security Erase, en utilisant la commande :

```
# hdparm -I /dev/sdX
```

Qui retourne, si ATA Security Erase est disponible, le résultat suivant (qui fournit aussi une évaluation de la durée de l'opération) :

```
[...]
Commands/features:
Enabled Supported:
* SMART feature set
* Security Mode feature set
[...]
114min for SECURITY ERASE UNIT. 114min for ENHANCED SECURITY ERASE UNIT.
[...]
```

Puis :

1. Il faut commencer par définir le mot de passe protégeant l'accès au disque pour les opérations de sécurité qui vont suivre. Pour ce faire on utilise la commande suivante :

   ```
   # hdparm --security-set-pass mot_de_passe /dev/sdX
   ```

Si le disque est en état frozen (aussi visible dans le retour de « hdparm –I »), comme parfois sur les portables, normalement toutes les commandes ATA Security sont bloquées. Il suffit de débrancher puis rebrancher le disque, ou de passer en veille pour le sortir de l'état « frozen » et exécuter la commande ci-dessus.

2. Effacement de sécurité (écrit des 0x00 ou des 0xFF sur tout le disque) :

```
#hdparm --security-erase mot_de_passe /dev/sdX
```

3. Si le disque est en état « frozen », passer l'ordinateur en mode veille, ou débrancher et rebrancher le disque (power cycle) pour l'en sortir.
4. Enfin, vérifier que le disque présente bien des 0x00 ou des 0xFF sur divers secteurs :

```
# hdparm --read-sector 0 /dev/sdX
[...]
# hdparm --read-sector XXXX /dev/sdX
[...]
```