Etude bas niveau de la mémoire et porte dérobée de VMware

Christian Abegg

IN3

19 avril 2010

Objectifs

- Mettre en œuvre un environnement s'exécutant en ring0 permettant de lire et d'écrire dans la mémoire vive sans restrictions.

- Etudier le fonctionnement de la porte dérobée de VMware

Explications des anneaux de protections

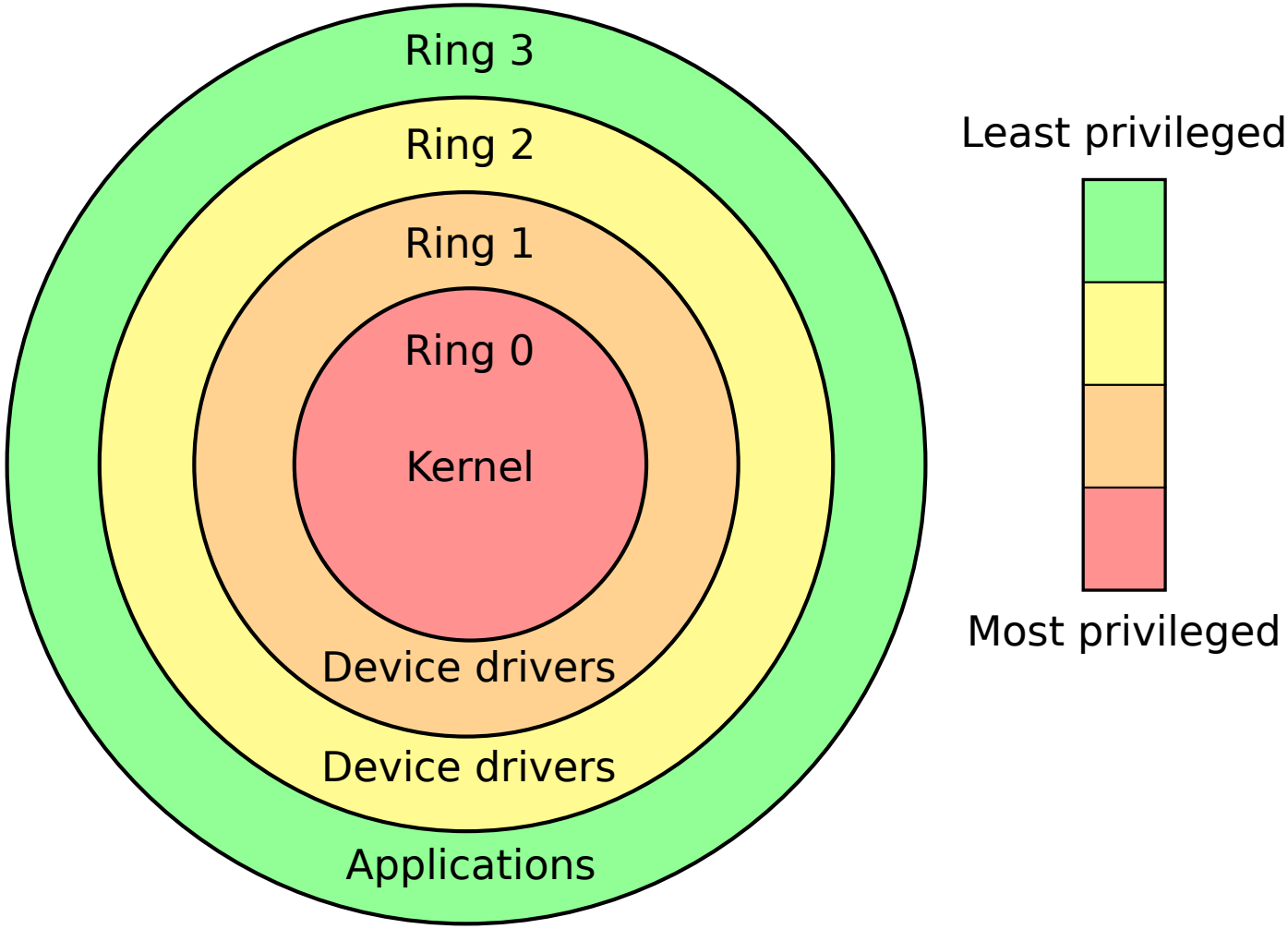

FIGURE: Anneaux de protections de l'architecture x86. Image tirée de Wikipédia : `http://en.wikipedia.org/wiki/File:Priv_rings.svg`

Analyse de la problématique

Accès mémoire

- La mémoire physique est partagée avec tous les systèmes invités
- Il faut une isolation
- Est-ce que la mémoire est initialisée avant qu'un système invité y ait accès ?

Porte dérobée VMware

- Représente un « canal de service »
- Permet à l'hyperviseur et à un système invité de communiquer
- Conçu pour la gestion de la souris, copie du presse-papier et ballooning mémoire

Isolation des machines virtuelles et de l'hyperviseur

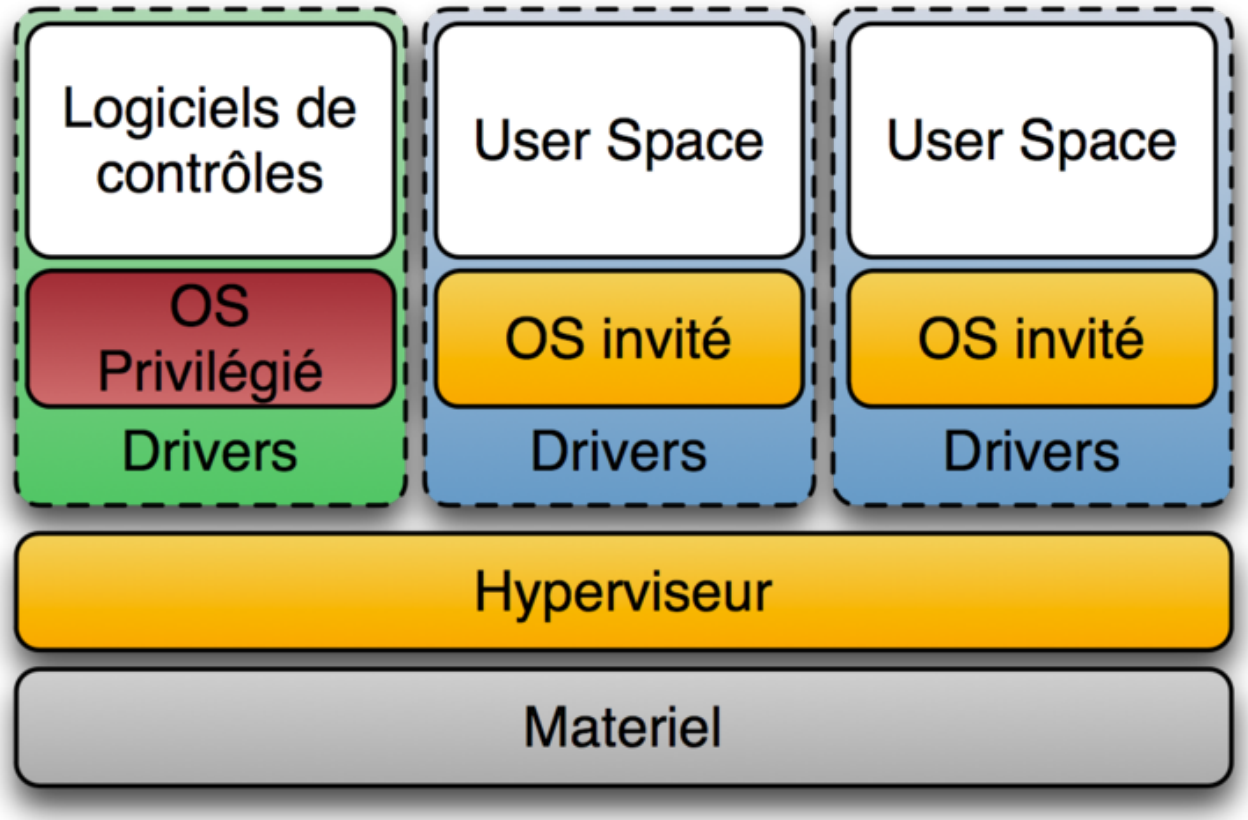

FIGURE: Architecture de virtualisation avec un hyperviseur. Image tirée de Wikipédia : `http://fr.wikipedia.org/wiki/Fichier:Diagramme_ArchiHyperviseur.png`

Accès mémoire

```
/* Définition d'un pointeur vers un char non signé */
unsigned char *addr = adresse;

/* Lecture de la case mémoire */
unsigned char valeur = *addr;

/* Ecriture dans la case mémoire */
*addr = 42;
```

Utilisation de la porte dérobée

```
/* Ecriture de la valeur magique dans l'accumulateur */
asm(" movl $0x564D5868, %eax; ");

/* Ecriture de la commande désirée dans le registre CX */
asm(" movw $0x0014, %cx;");

/* Choix du port I/O de VMware dans le registre DX */
asm(" movw $0x5658, %dx;");

/* Lecture du port I/O */
asm(" inl %dx, %eax;");

/* Lecture de l'accumulateur contenant la taille de la RAM */
asm(" movl %%eax, %0;" :"=r"(mem));
```

Démarrage d'un système d'exploitation

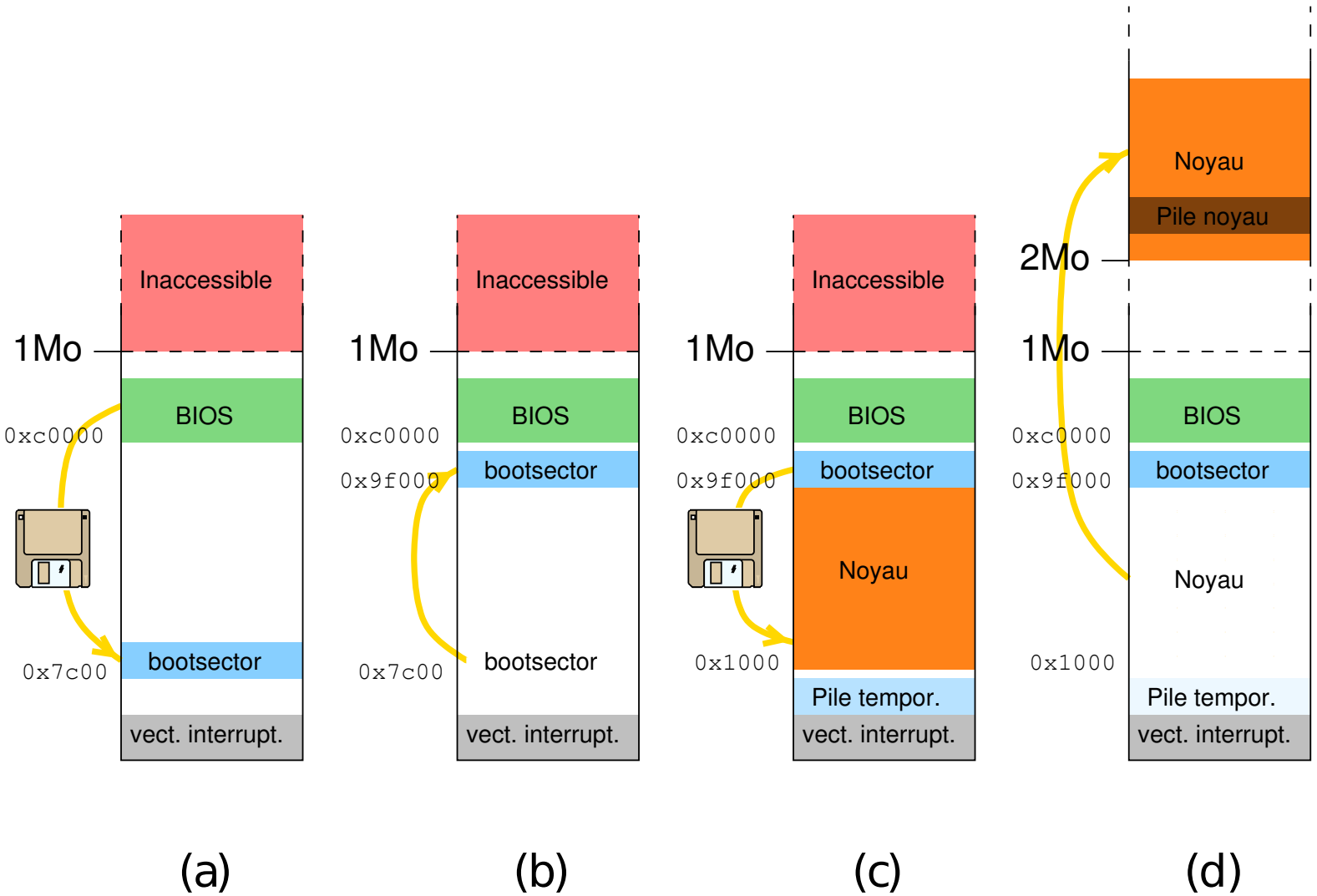

FIGURE: Etapes de chargement du noyau par le secteur d'amorce. Source : Article 1 de SOS

Démonstration

- Comportement de la mémoire
  - dans une machine virtuelle
  - avec une machine physique

- Méthodes de la porte dérobée

Conclusion

- Vérification par la pratique que VMware initialise la mémoire vive avant tout accès du système invité

- Confirmation de l'existence de la porte dérobée incluse dans VMware, des informations sur l'hyperviseur ont pu être récupérées

Questions/Réponses, Références

Intel Software Developer's Manuals

`http://www.intel.com/products/processor/manuals/`

Wikipédia

`http://www.wikipedia.org/`

Ken Kato.

VMware Backdoor I/O Port

`http://chitchat.at.infoseek.co.jp/vmware/backdoor.html`

Pierre Maurette

Assembleur

Micro Application, 2003

David Decotigny & Thomas Petazzoni

Croisière au cœur d'un OS

`http://sos.enix.org/`

Test mémoire avec VMware

Test mémoire avec VMware

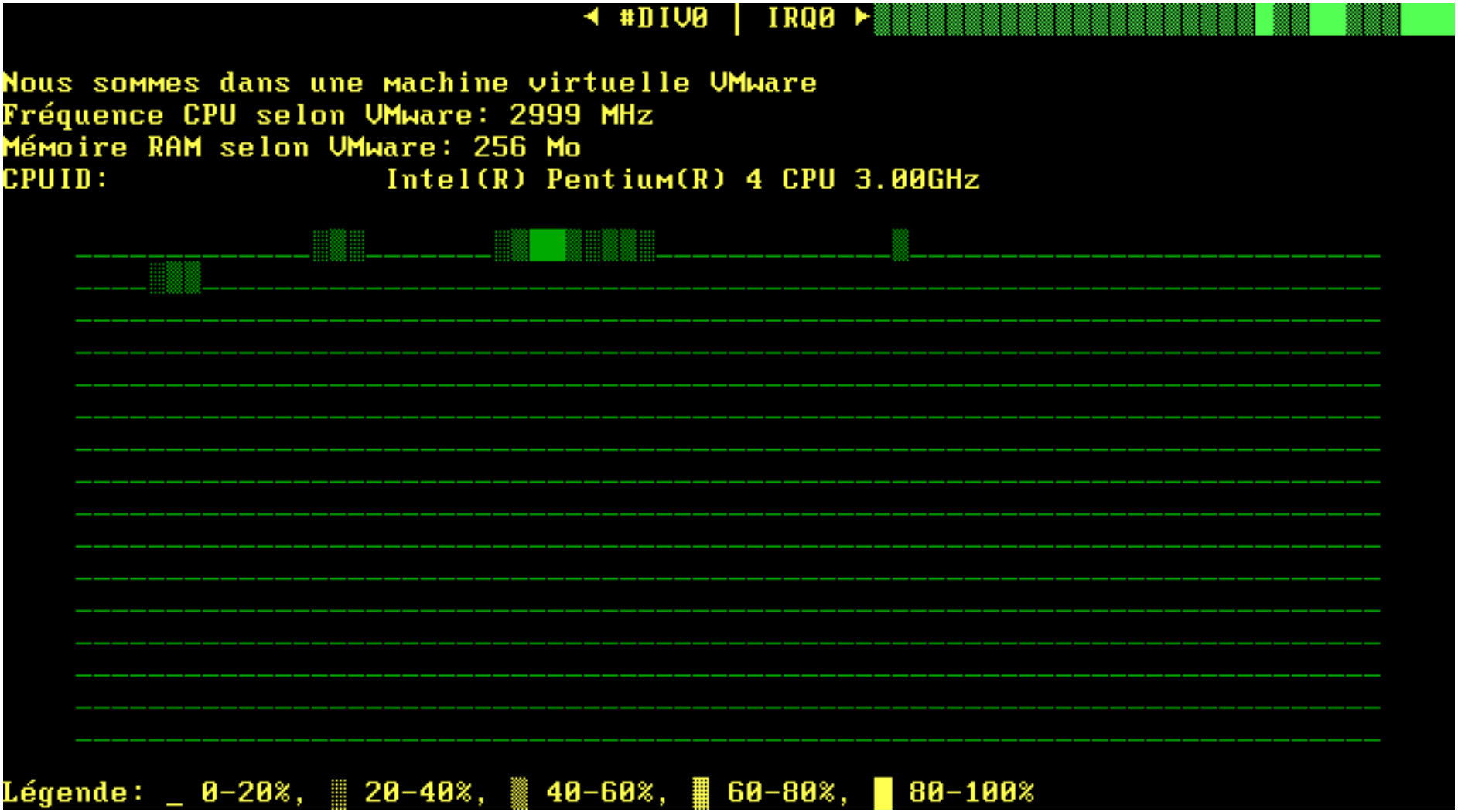

FIGURE: Etat de la mémoire vive avant écriture

Test mémoire avec VMware

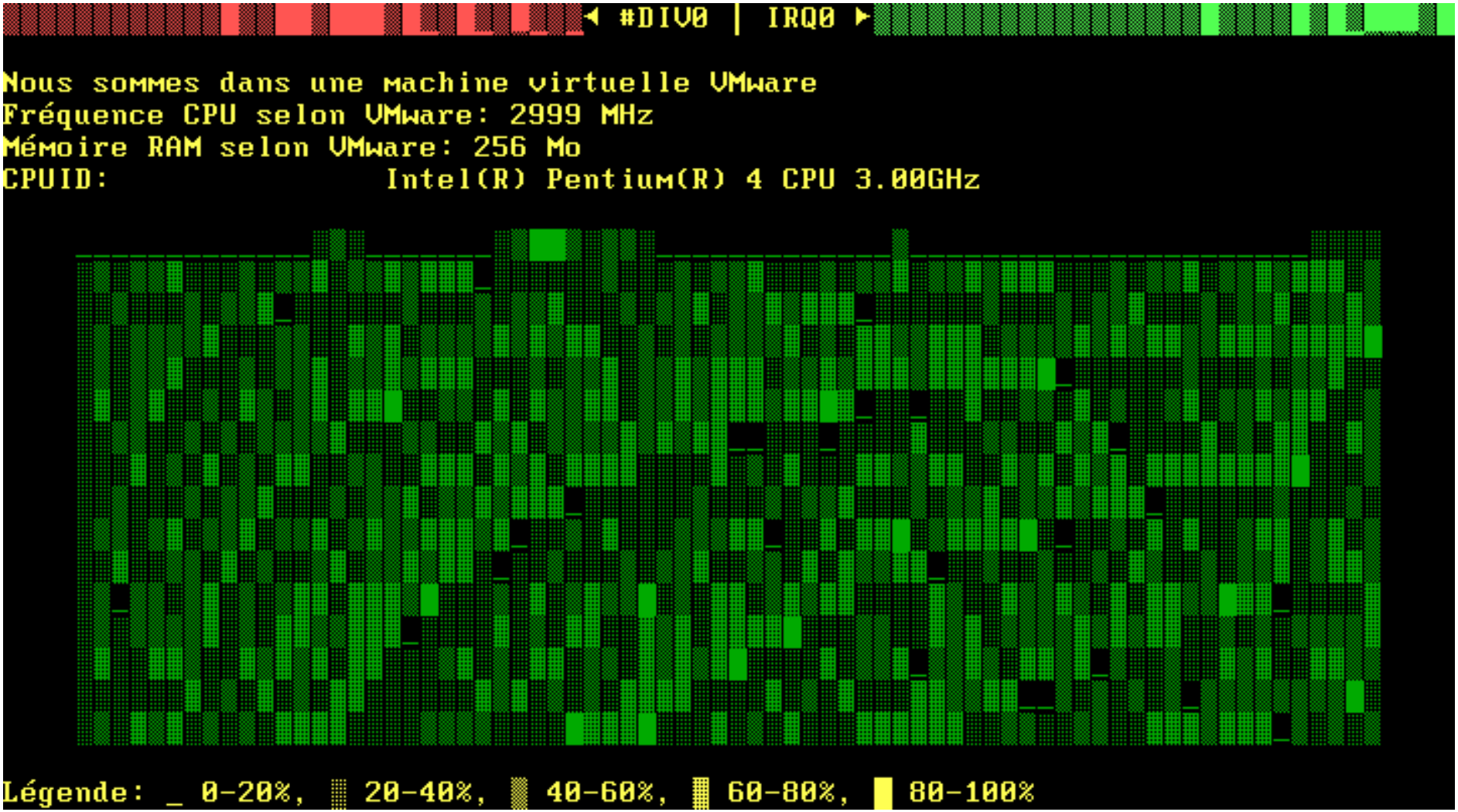

FIGURE: Etat de la mémoire vive après écriture

Test mémoire avec un PC IBM

Test mémoire avec un PC IBM

FIGURE: Etat de la mémoire vive avant écriture, après démarrage à froid

Test mémoire avec un PC IBM

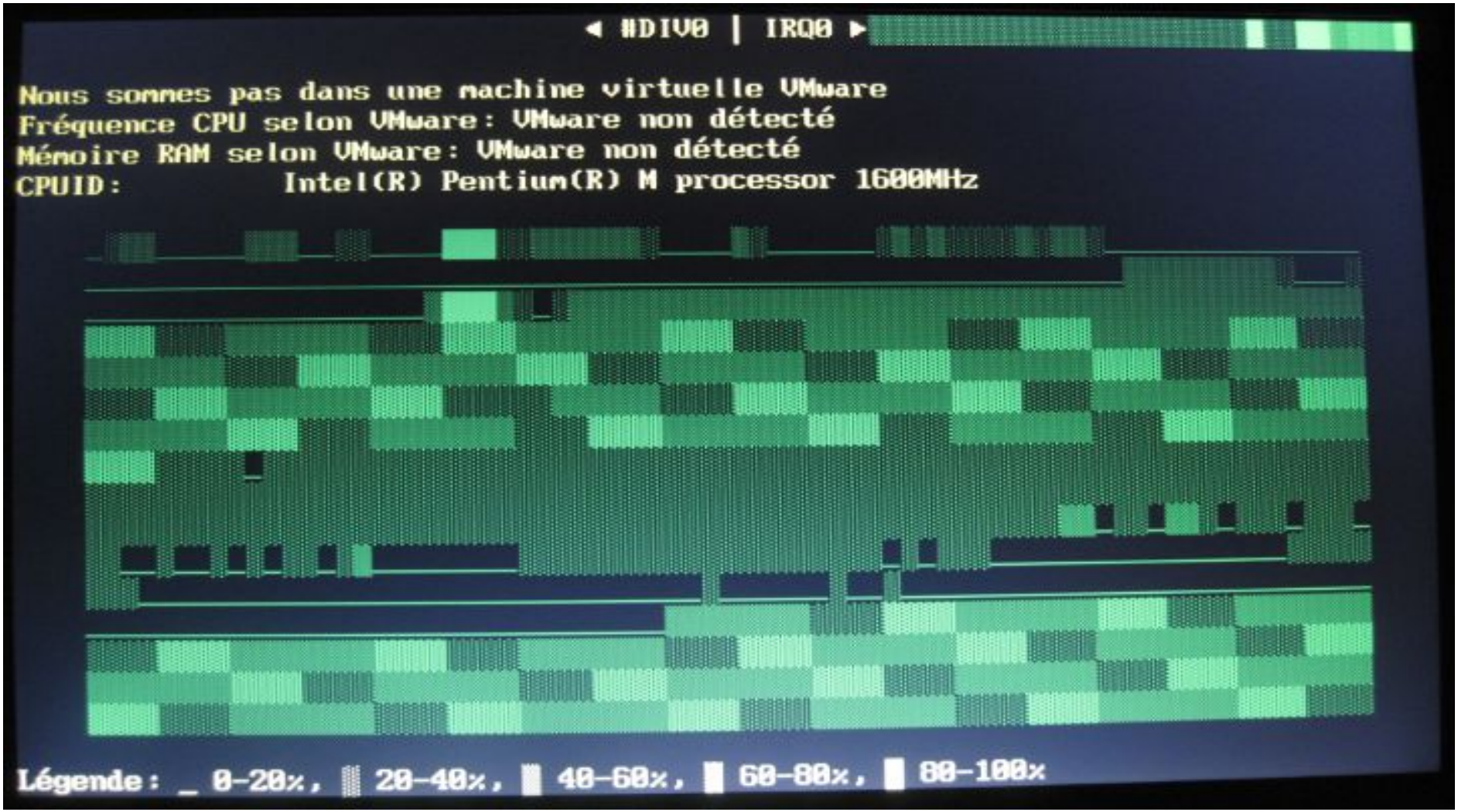

FIGURE: Etat de la mémoire vive avant écriture, mais après redémarrage à chaud depuis Linux

Test mémoire avec un PC IBM

FIGURE: Etat de la mémoire vive après écriture

Test mémoire avec un PC IBM

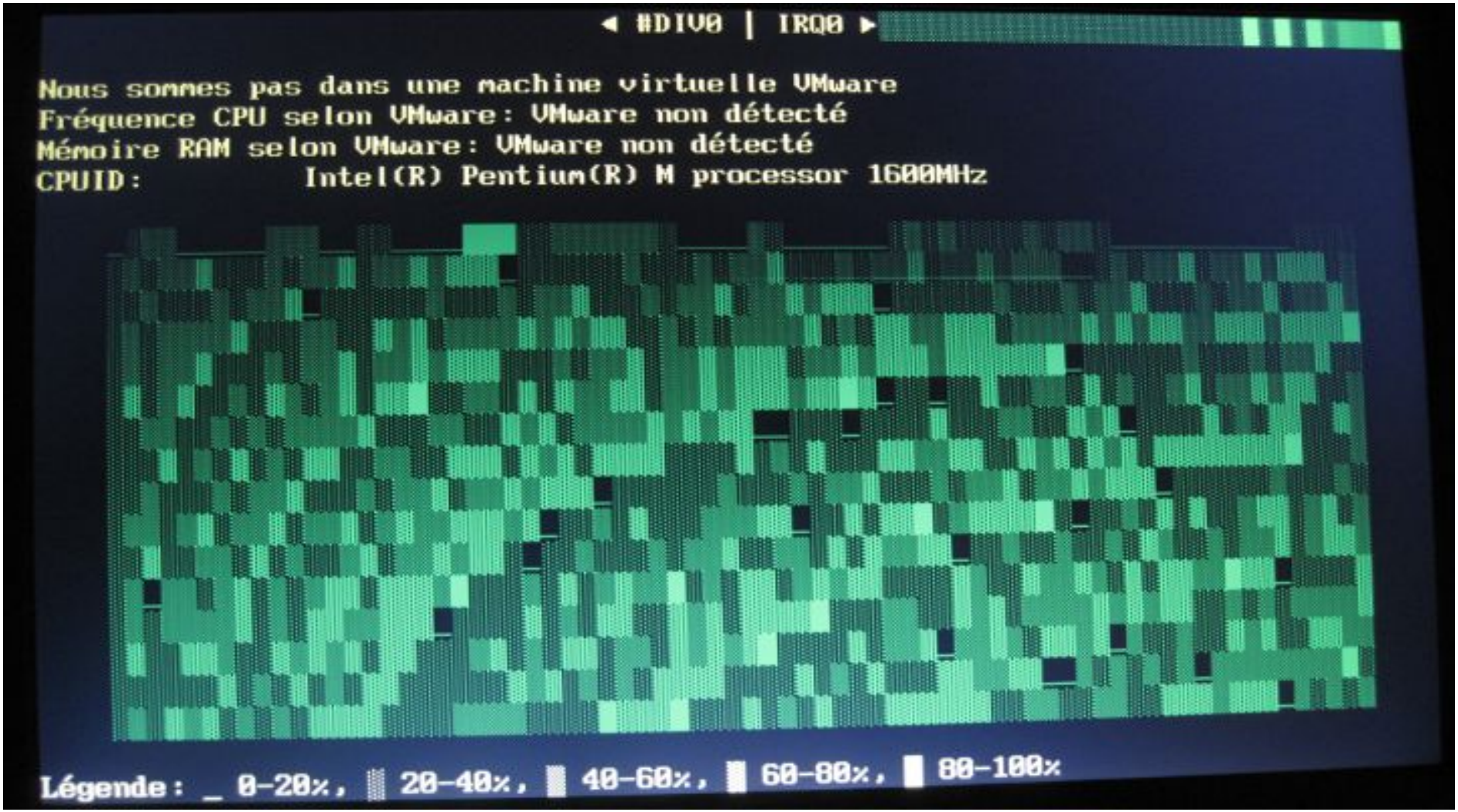

FIGURE: Etat de la mémoire vive après écriture, arrêt de la machine pendant 30 s. La mémoire n'a pas changé.