# Indiscrétions et « zones constructeurs » des disques durs

Laurent Dupuy

FreeSecurity
sstic-ld@freesec.net

**Résumé** Aujourd'hui, les disques durs sont de véritables boîtes noires. Ils intègrent des contre-mesures logicielles au coeur même de la carte de gestion de chaque support de stockage. De nombreux constructeurs ou éditeurs de logiciels utilisent ces moyens pour limiter ou contrôler l'usage du support de stockage et ainsi protéger la propriété industrielle des oeuvres numériques.

Quels sont ces types de protection, quels sont aujourd'hui leurs niveaux de solidité face aux moyens d'analyse publiquement disponibles ? Une première réponse sera apportée lors de la presentation notamment par une exploration des modules presents au coeur des « zones constructeurs » appuyée par une revue des modes de fonctionnement et des méthodes de protection définies dans la norme ATA.

## 1 Problématique

Les disques durs sont des supports de stockage devenus classiques dans la vie moderne, ainsi il est possible de trouver ce bout de metal dans tous équipements : du baladeur numérique à la console de jeux video en passant par l'ordinateur portable du directeur. Dés lors, des informations confidentielles tant pour le particulier que pour l'entreprise se retrouvent soumises à un environnement extérieur potentiellement « dangereux ». Ces derniéres anées les disques durs donnent toutes latitudes aux entreprises pour protéger leurs contenus ainsi le verrouillage des logiciels presents sur le disque dur, la limitation de l'espace de stockage ou la creation de zone sécurisé hors d'atteinte de l'utilisateur sont très commodément configurables.

Il est facile de constater que les aspects « sécurité », longtemps sous utilisés des disques durs sont maintenant largement employés. Dés lors, réalisé une simple copie de sauvegarde, accéder à ses données sans utiliser le logiciel « propriétaire » du fabriquant ou recycler un materiel verrouillé devient une opération de plus en plus complexe pour l'utilisateur final.

## 2 Les zones constructeurs

L'on peut identifier plusieurs zones constructeurs sur un disque dur comme les G-list, P-list, HPA, DCO, ou encore FIRMWARE chacune de ces zones possédent des caractéristiques et des objectifs différents.

Dans le cas des P-list par exemple cette zone à pour but de garder en mémoire les secteurs défectueux sur le disque lors de sa sortie de l'usine à contrario de la P-list qui quant á elle conserve les secteurs defectueux rencontré suite à la sortie de l'usine. Il devient évident que la modification de ces tables permet de cacher plus ou moins efficacement de l'information, voir de la rendre résistante à un effacement même sécurisé.

De plus, l'accès à ces zones défectueuses est normalement supprimé par le contrôleur de disque dur, seul des commandes constructeurs peu documentées ou des outils spécifiques permettent de lire ces informations.

## 3 La norme ATA

La norme ATA mise en place est maintenue par INCITS, les commandes définies dans la norme (ATA 8) permettent au contrôleur de piloter le disque dur. Les commandes à destination des disques S-ATA et PATA sont différentes, seules les commandes PATA sont évoquées dans cet article.

La norme ATA permet de connaître l'ensemble des protocoles de commandes nécessaire au pilotage du disque. Cependant la reprogrammation du FIRMWARE est propre à chaque fabriquant et reste confidentielle.

## 4 Les technologies de protections

Dans les chapitres suivants, les méthodes de protections classiques utilisées par les éditeurs de logiciels ou les fournisseurs de solutions seront exposées.

### 4.1 Le numéro de série materiel

Le numéro de série du disque dur est utilisé dans de nombreux systèmes de licence permettant de lier le materiel au logiciel, ainsi, tout changement du disque dur entraînera la nécessite d'une nouvelle licence. Le numéro de série materiel du disque dur est une donnée stockée dans la zone constructeur.

### 4.2 Les mots de passe

Le mot de passe « utilisateur » du disque dur présenté par certains, comme « la » sécurité de l'ordinateur portable consiste à mémoriser directement sur le disque dur (system area) ou dans une EEPROM une chaîne de caractère permettant d'accéder au contenu du disque. Des lors, le disque dur ne peut démarrer sans ce mot de passe. selon le niveau de sécurité choisi respectivement « high » ou « maximum » le comportement du « master » password change permettant soit de déverrouiller le disque dur comme le mot de passe utilisateur, soit si le mot de passe « utilisateur » n'est pas connu, il permettra uniquement de réaliser un effacement sécurisé (voir theme suivant).

Cette technique de protection est utilisée dans les consoles de jeux, dans certains ordinateurs portables, elle est souvent mêlée aux systèmes de lecture d'empreintes digitales.

### 4.3 L'effacement ATA

La norme ATA permet d'utiliser deux types d'effacement le « normal erase mode » qui écrase le contenu du disque avec des zeros en respectant la zone hpa (et dco ?) et le « enhanced erase mode » permettant d'effacer completement le disque en écrasant les données avec une chaîne de caractère définie.

### 4.4 La zone HPA

La zone HPA (host protected area) est une fonctionnalité permettant de créer une zone normalement non accessible par l'utilisateur. Des lors, le nombre de secteur du disque dur est artificiellement réduit. Plus souple que la zone DCO ci-dessous, la zone HPA peut être désactivée uniquement en mémoire vive ou directement dans la mémoire de masse.

Cette technologie est utilisée par exemple pour restaurer le système d'exploitation. Cette pratique est courante sur les portables ou les ordinateurs livrés sans CD-ROM d'installation.

### 4.5 La zone DCO

La zone DCO (Device configuration overlays) permet de créer un disque dur de même caractéristique qu'un disque dur ayant une capacité inférieure et fabriqué par un autre constructeur. Par ricochet, il est ainsi possible de créer une zone protegée sur le disque dur, cette technique reste cependant moins usitée, tout en étant detectable lors d'une autopsie de disque.

L'utilisation de ces fonctionnalités pourrait permettre à un utilisateur de cacher au yeux d'un expert judiciaire des informations sensibles. Cependant, l'utilisation d'outils de copie avancés permet de détecter l'activation de ces contre-mesures.

## 5 Les attaques

Les thémes ci-dessous présentent un resumé des attaques possibles sur les protections classiques des disques durs, abordés plus en detail lors de la présentation du sstic.

### 5.1 La reprogrammation du « firmware »

L'analyse à porté sur un disque dur référence Maxtor DiamondMax Plus9 « calypso » . Ce disque, un peu ancien, présente l'avantage d'être bien documenté, les modules de son firmware ne présentent que peu de point d'ombre.

Les principales informations contenues dans les zones constructeurs d'un disque dur maxtor « calypso » :

- l'encodage et la structure des secteurs,
- les données destinées au « servomoteur »,
- la géométries du disque,
- les tables de zones défectueuses,
- la structure du firmware,
- l'identité du disque dur.

Les fichiers de firmware permettent de reprogrammer tout ou partie d'un disque dur. Ces fichiers sont composés en général du boot loader extension par défaut .ldr, du firmware .Ram et des modules. La taille totale des fichiers est d'environ 7 Mo.

Les zones clefs impactées par une reprogrammation compléte du disque sont les suivantes :

- les zones P-list et G-list,
- les mots de passe master et user,
- la gestion SMART,
- le passeport du disque dur (modèle, numéro de série,

Ce type d'approche permet avec plus ou moins de manipulation selon les modèles de disque dur de « défaire » les protections HPA, DCO ou par mot de passe.

En figure 1, ci-après, la photographie présente les composants clefs de la carte électronique :

Il est ainsi possible de retrouver de gauche à droite les composants suivants : ST25P10V6, SH6782B, FDS9431A, 2125G W981616BH-6, Ardent C5.

### 5.2 Les attaques en « Force Brute »

Les attaques en brute force sont longues et fastidieuses, un compteur d'essai infructueux est present sur le disque nécessitant le re-demarage de ce dernier toutes le cinq tentatives erronées.

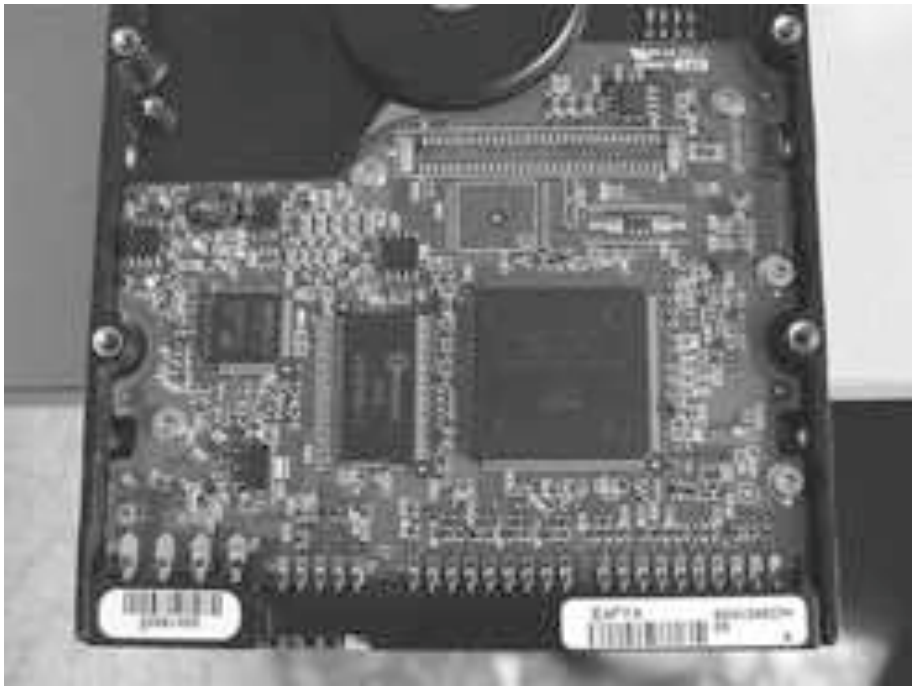

FIG. 1: Maxtor Calypso III

### 5.3 Suppression matérielle des securités

Selon le modèle de disque dur le changement complet de la carte électronique permet de supprimer la notion de mot de passe. Cependant, les disques doivent être de la même série. Les constructeurs ayant l'habitude de faire fabriquer leurs disques durs dans le monde entier, de nombreux disques durs de même modèle possèdent des cartes mêres assez différentes.

## 6 Conclusion

L'analyse du mode de fonctionnement des disques durs est un vaste sujet nécessitant des outils encore confidentiels ou très onéreux. La compréhension de ces aspects permet de mieux cerner et d'accorder une confiance pour le moins limitée aux méthodes de protection correspondant à la norme ATA utilisée actuellement pour verrouiller les disques durs des ordinateurs.

La regénération des zones fabricants d'un disque dur dépasse le cadre pur de la sécurité pour permettre la récuperation avancée des disques durs mêlant souvent un disque dur « fonctionnel » jouant le rôle de donneur dans le but de rendre fonctionnel un disque défaillant recevant les piéces détachées.

## Remerciements

Je tiens à remercier Philippe Biondi pour sa patience ainsi que les relecteurs.