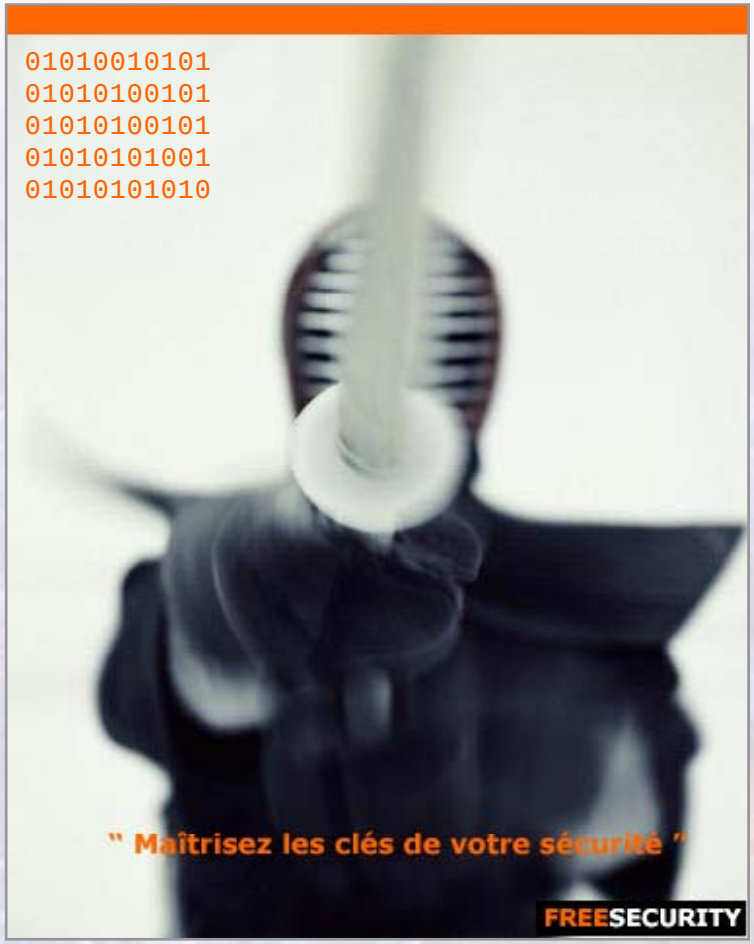

Indiscrétions et « zones constructeurs »
« Redécouvrons nos disques durs »
FREESECURITY™

Agenda

- Problématiques,
- Le disque dur,
- Les « zones constructeurs »,
- La norme ATA,
- Les techniques de protection,
- Les attaques possibles,
- Conclusion & recommandations,



Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

La problématique

- Comment protéger matériellement les données d'un ordinateur ?,
- Quelle est la meilleure solution pour lier matériel et logiciel à moindre coût ?,
- Comment permettre un effacement « rapide » des données du disque dur ?,
- Quelle est la solution pour bloquer l'accès aux données ?.

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Réponse classique :

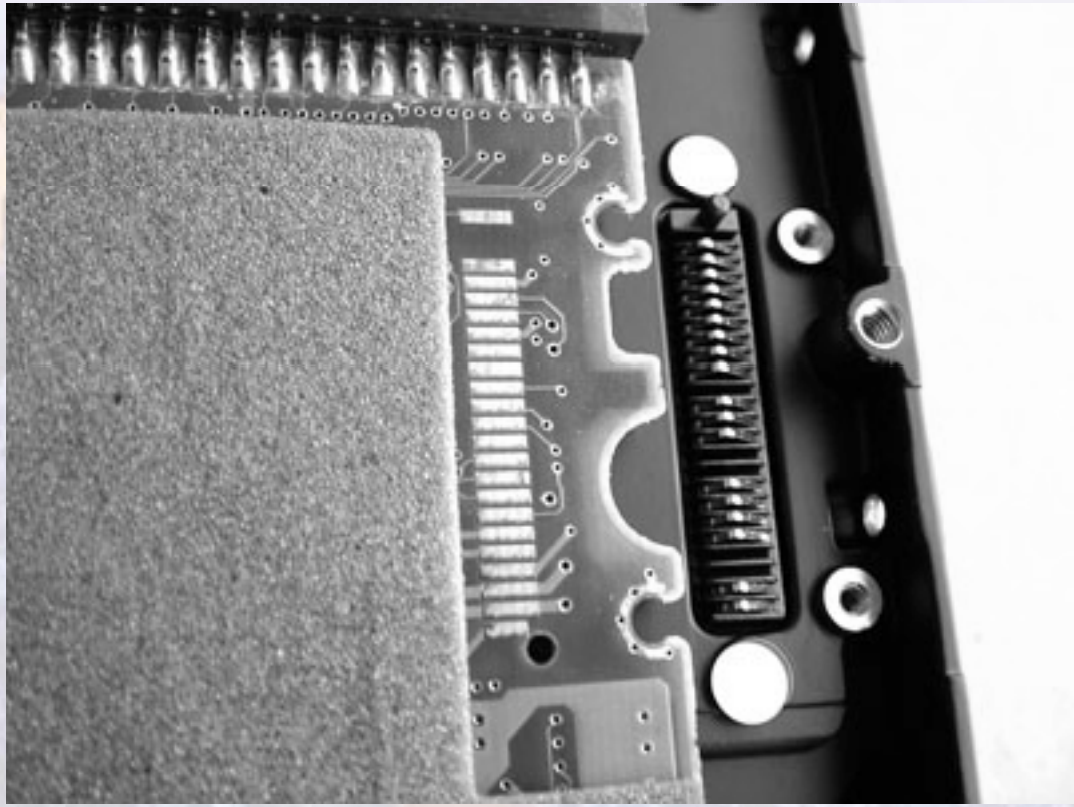
- Le disque dur informatique :
  - Module matériel pratiquement présent dans tous les ordinateurs,
  - Il est la première brique en contact avec les données,
  - Il est composé d'un logiciel embarqué spécifique à chaque constructeur,
  - Il contrôle l'accès aux données du disque.

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Description d’un disque dur contemporain

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Description d’un disque dur contemporain



Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Description d’un disque dur contemporain

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Description d’un disque dur contemporain

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Description d’un disque dur contemporain

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

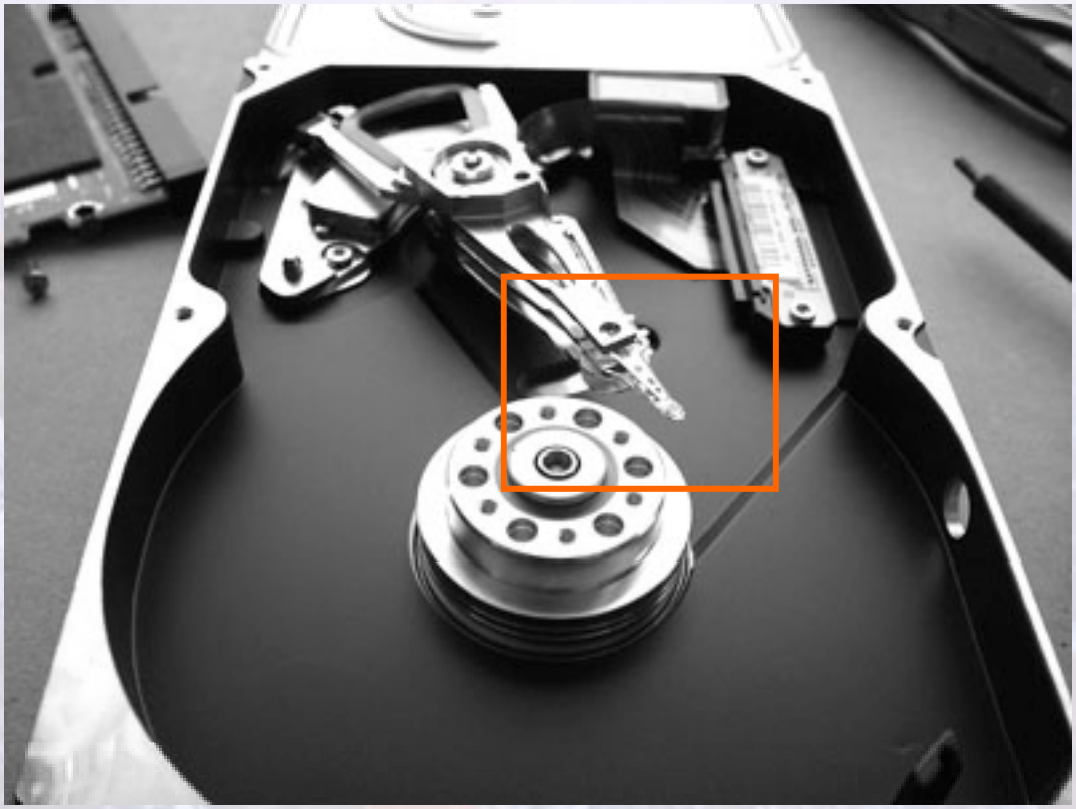
Description d’un disque dur contemporain

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Description d’un disque dur contemporain

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Description d’un disque dur contemporain

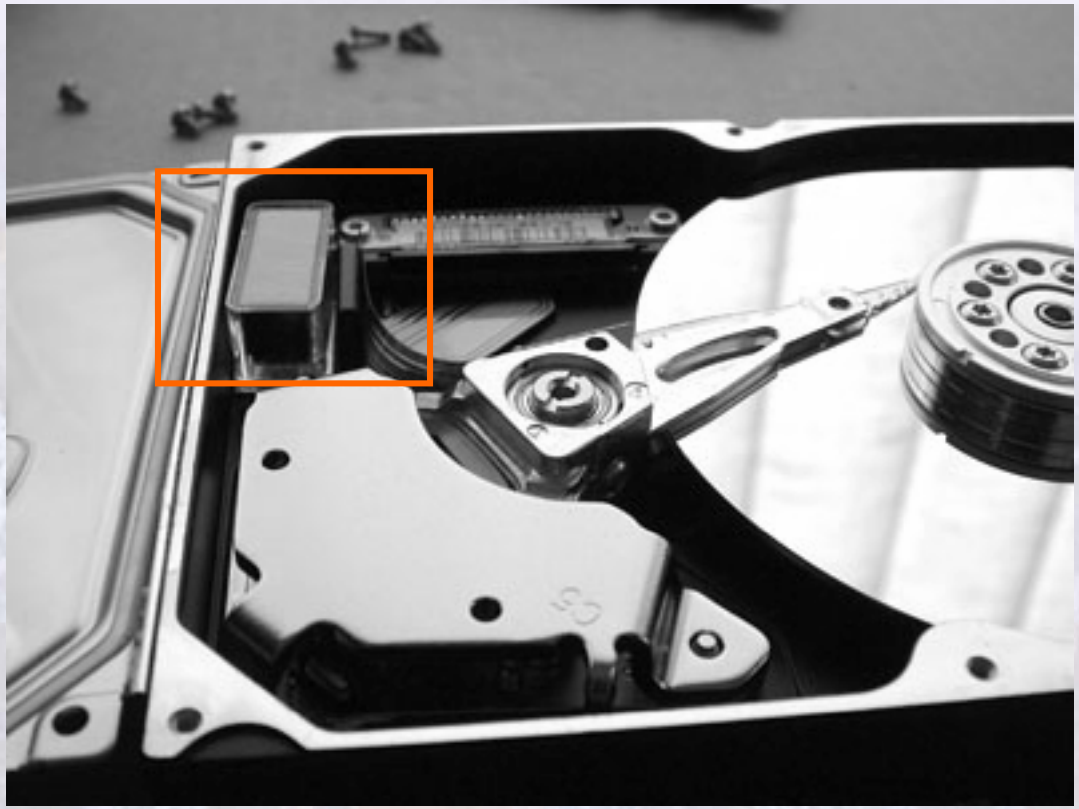


Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Description d’un disque dur contemporain

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Description d’un disque dur contemporain

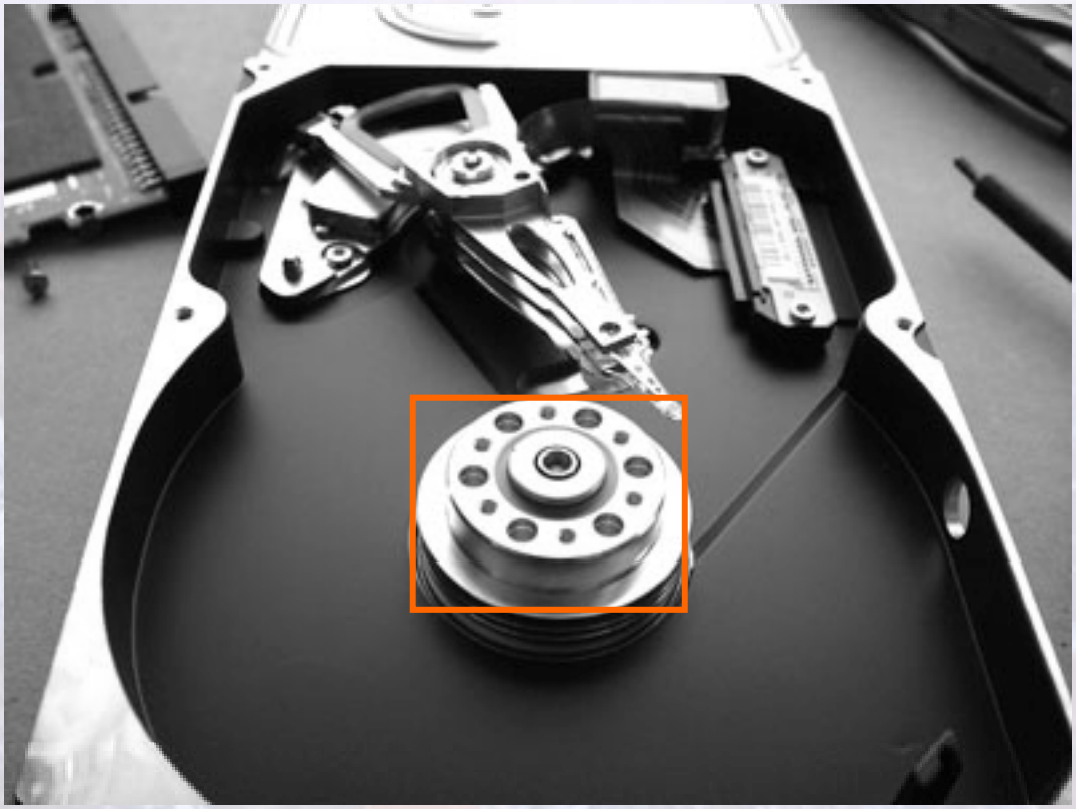


Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Description d’un disque dur contemporain

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Description d’un disque dur contemporain

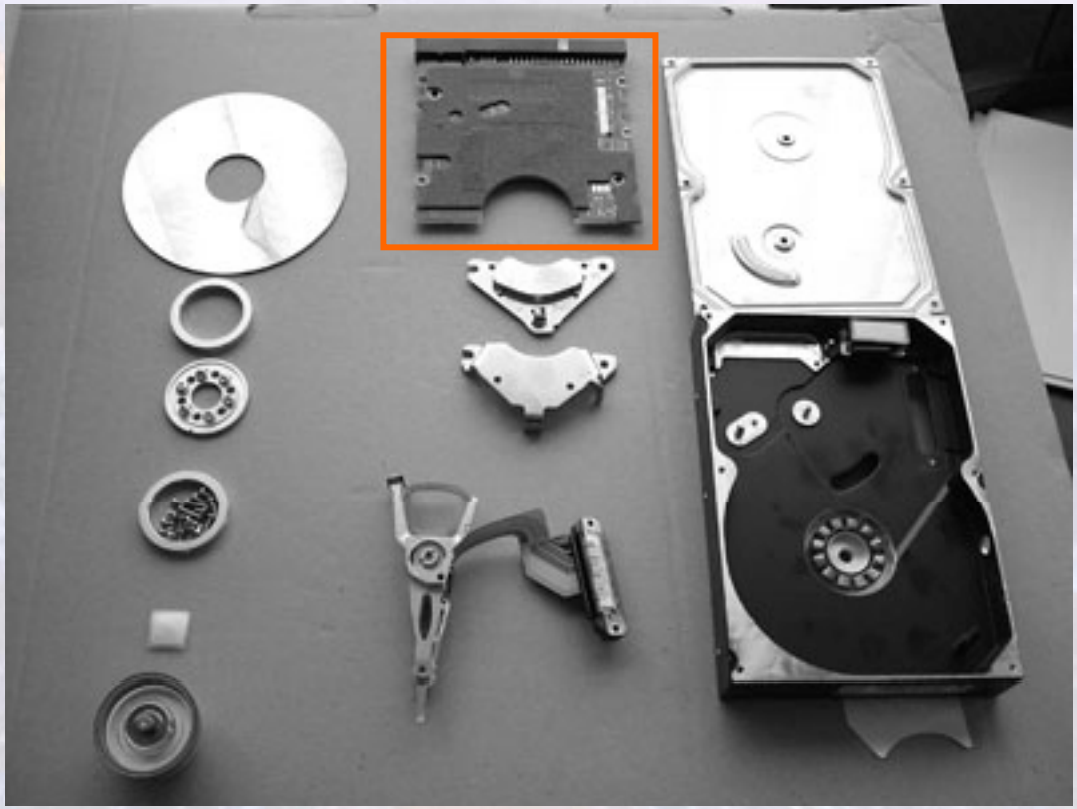


Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Description d’un disque dur contemporain

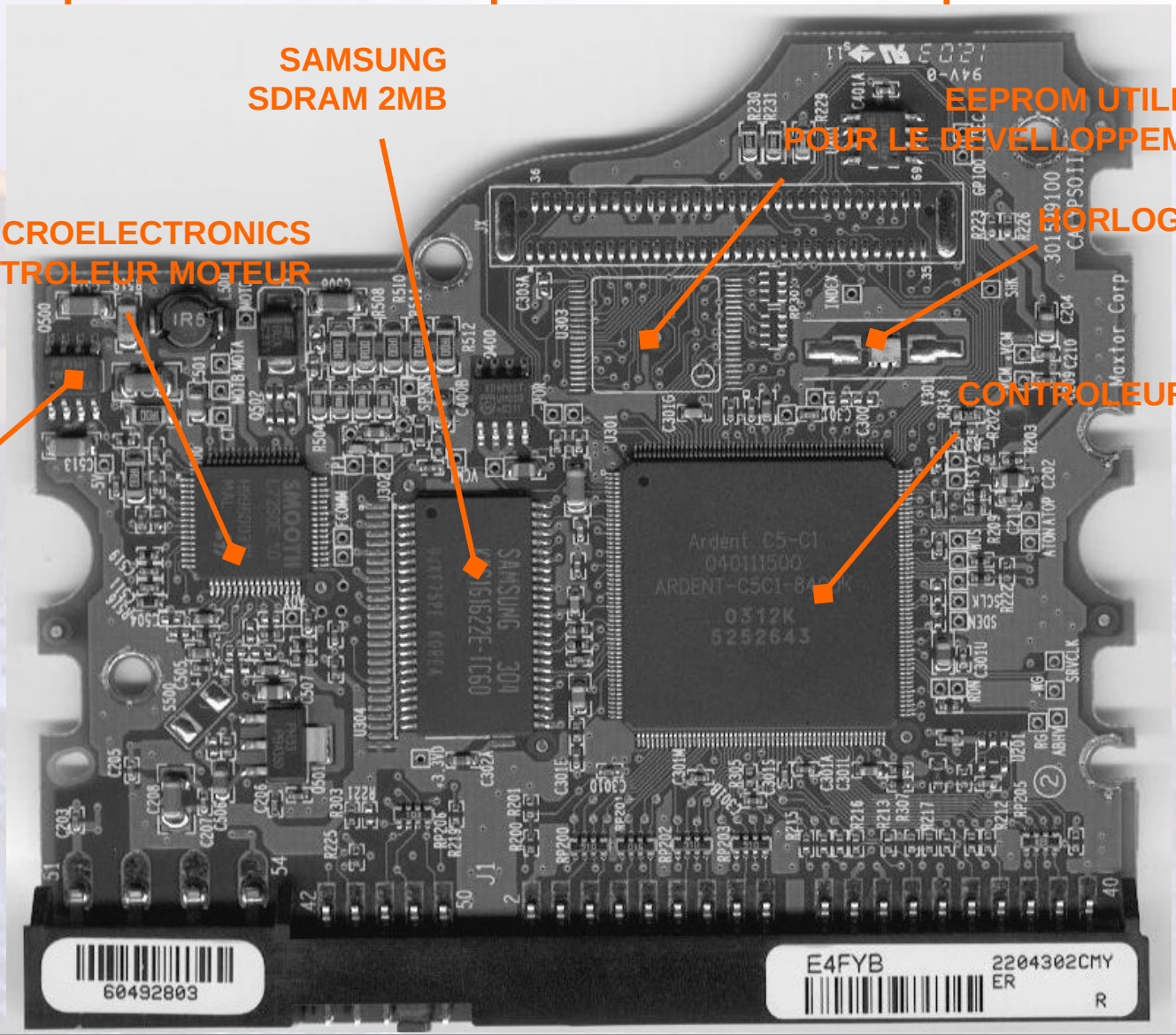
Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Description d’un disque dur contemporain



Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Description d’un disque dur contemporain



Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Les zones constructeurs

- Il existe plusieurs zones constructeurs ou modules sur un disque dur contenues dans un secteur du disque non adressable par l'utilisateur : la « system area » SA.

- On y retrouve par exemple :
  - Le Firmware du disque,
  - La table des secteurs défectueux (G-list),
  - Les informations « SMART »,
  - Le mot de passe du disque.

- Il est nécessaire d'utiliser des commandes constructeurs « souvent non documentées » pour arriver à ces zones.

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Les zones constructeurs

- L'information est présente dans un cylindre du disque dit « négatif » qui n'est pas accessible par les commandes « read » standard.

- Il existe quelques outils permettant de réaliser des opérations de lectures/écritures pour des prix allant de 100€ à plus de 5000€.

  PC3000

  Création d'un contrôleur à base de µPIC

  IdeGRABB

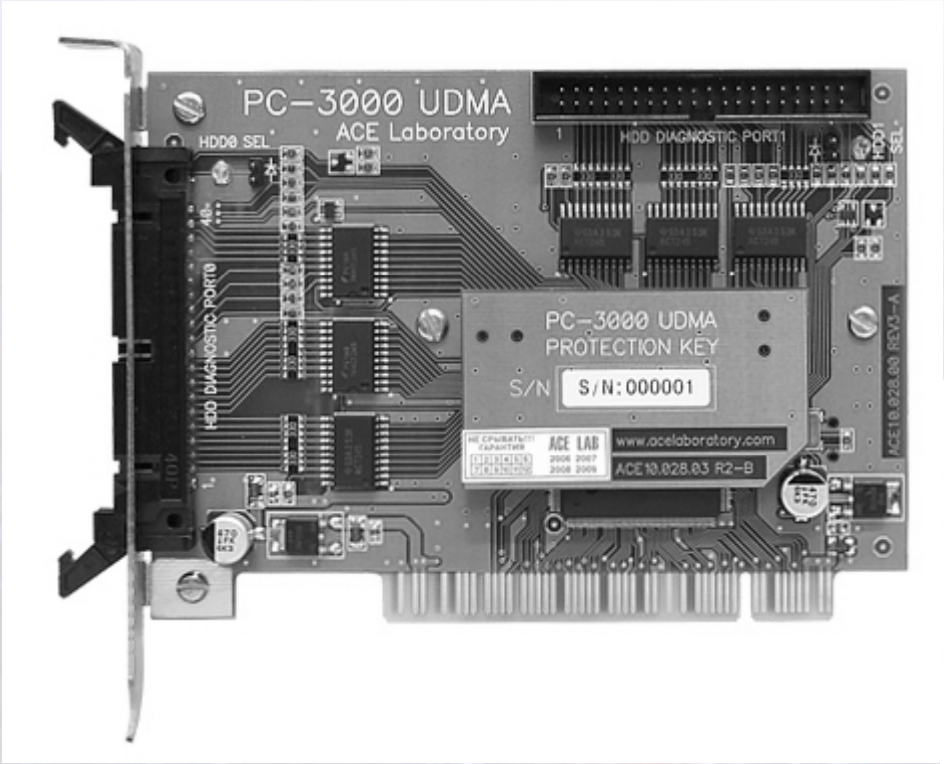
- La clef de voûte repose sur la connaissance des commandes des constructeurs (IBM,Hitachi,…).

- Et une piste que nous voulons explorer à termes :

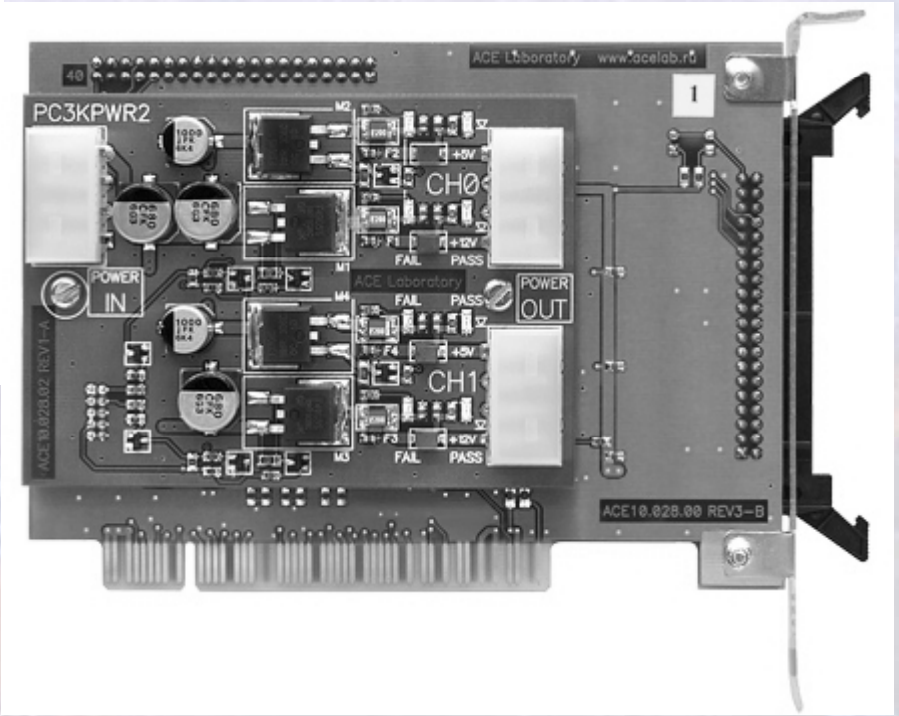
  Windows Server 2003 et XP avec SP2 (IOCTL_ATA_PASS_THROUGH)

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Les zones constructeurs



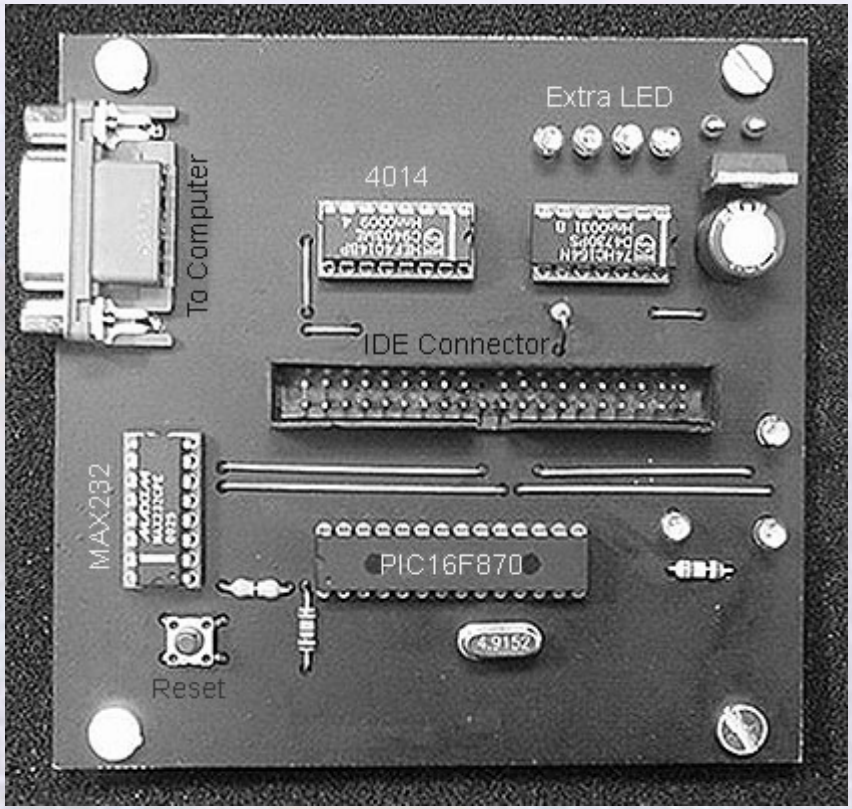
PC3000



Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Les zones constructeurs

DIY CONTROLEUR DISQUE DUR



Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Les zones constructeurs

- Descriptif de quelques zones intéressantes :

  La P-LIST, ce module contient les secteurs défectueux rencontrés en usine.

  La G-LIST, cette liste contient les secteurs découverts au cours de la vie du disque dur.

  Firmware, il contient le microcode du disque dur lui permettant de fonctionner

  N° de série matériel du disque

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

La norme ATA

- Elle permet d'avoir un socle commun de commande pour tous les disques durs du marché, seul l'accès aux zones constructeurs est conservé confidentiel par les fabricants.

T13/1699D Revision 2b – 10 janvier 2006

CHECK POWER MODE	Executable	Executable	Executable
CONFIGURE STREAM	Command aborted	Executable	Executable
DEVICE CONFIGURATION	Command aborted	Executable	Executable
DEVICE RESET	Executable	Executable	Executable
DOWNLOAD MICROCODE	Vendor Specific	Vendor Specific	Vendor Specific
EXECUTE DEVICE DIAGNOSTIC	Executable	Executable	Executable
FLUSH CACHE	Command aborted	Executable	Executable

- Si vous êtes intéressé c'est avec plaisir que je vous transmettrez ces documents,

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

La norme ATA

- Les commandes sont ainsi reçues par le port PATA du disque et exécutées par le contrôleur.

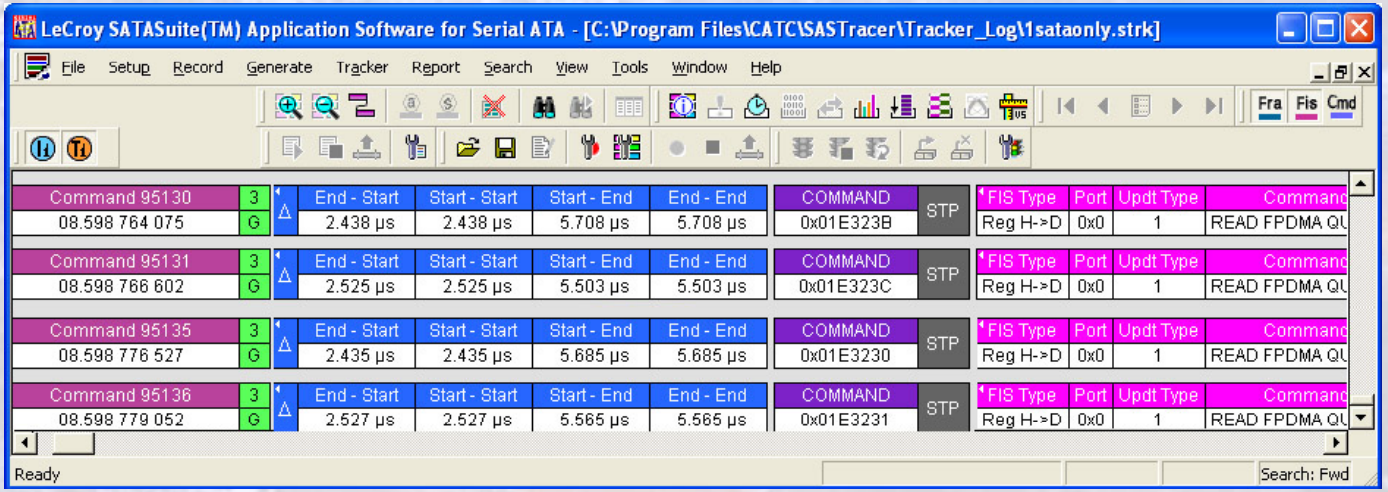
Contrôleur ou interface spécifique

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

La norme ATA

- Pour aller plus loin avec la norme SATA des outils sont indispensables, mais pour l'instant hors d'atteinte, car très onéreux.

SataTRACKER



Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Les technologies de protection

- Aujourd'hui le disque dur joue le plus souvent le rôle d'une clef protégeant une partie ou la totalité des informations utilisées par les éditeurs de logiciels.

- Certaines sociétés basent la protection de leurs postes nomades sur la sécurité du mot de passe intégré au disque dur.

- Quels sont les moyens et les menaces associés à ces pratiques ?

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Les technologies de protection

- Le numéro de série matériel

  Il permet de lier de façon définitive par exemple un logiciel à un composant matériel (qui de surcroît tombe normalement en panne tous les 3 à 4 ans),

  Un numéro de licence intermédiaire est communiqué au fabriquant qui adresse en retour la clef de déverrouillage. Le logiciel de l'éditeur vérifiera systématiquement que la clef correspond au matériel présent dans l'ordinateur.

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Les technologies de protection

- Le mot de passe (disque dur) :

  Il est utilisé par des grands fabricants d'ordinateur portable,

  Cette protection consiste à mémoriser le mot de passe dans la zone SA du disque dur, dés lors, aucun démarrage n'est « possible » sans demande de mot de passe.

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Les technologies de protection

- Le mot de passe (disque dur) :

  Il existe (Draft jan 06) deux mots de passe pour protéger le disque dur d'un ordinateur et deux modes de fonctionnement.

  Le mot de passe « MASTER » permet de déverrouiller le disque dur en cas de perte du mot de passe « USER »

  - En cas d'un mode de fonctionnement « High », le disque dur sera déverrouillé,
  - En cas de fonctionnement « Maximum », le disque sera effacé totalement et déverrouillé.

  Dans tout les cas, lors de la configuration on utilisera la commande « SECURITY FREEZE LOCK » pour empêcher la modification du mot de passe.

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Les technologies de protection

- La zone HPA :

- Host protected area, est une fonctionnalité créant une zone non accessible par l'utilisateur

  Cette approche permet de modifier artificiellement la taille du disque directement en mémoire vive,

  Ce type de fonctionnement a déjà été rencontré dans des systèmes d'enregistrement vendus sur le marché américain avec un disque de 120 Go, mais ne laissant accessible coté utilisateur que 40 Go. Un « upgrade » payant permettait ainsi de passer à 80 ou 120 Go.

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Les technologies de protection

- La zone DCO :

- Device configuration overlay, permettant de créer un disque dur ayant les mêmes caractéristiques qu'un disque de taille inférieure.

  Ainsi, il est possible de fournir à un client des disques de capacités similaires pourtant non fabriqués aujourd'hui,

  ou de masquer aux yeux d'une analyse classique le contenu du disque.

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Les technologies de protection

- L’effacement ATA :

  Le microcode présent sur le disque dur permet de lancer un effacement sécurisé du support,

  ainsi un disque équipé d’une petite carte avec un microprocesseur PIC et d’une batterie pourrait rentrer en mode d’effacement de façon autonome même si le courant est coupé, garantissant ainsi un effacement au maximum de la vitesse du support.

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Les contre-mesures et attaques possibles

- Comment un attaquant peut modifier le N° de série d'un disque dur ?
- Quelle est la solution utilisée pour supprimer une zone HPA ou DCO ?
- Comment est-il possible pour un attaquant de supprimer le mot de passe d'un disque ?

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Réponse

- Les attaques sur les moyens de protection vues précédemment sont possibles via des commandes non documentées,

- Ces commandes sont complétées par des actions (contacts) sur le circuit imprimé du disque dur.

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Les contre-mesures et attaques possibles

- Suppression du mot de passe

  Dans cette phase, on mêle base de connaissance avec des actions matérielles sur le disque

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Les contre-mesures et attaques possibles

- Suppression du mot de passe

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Les contre-mesures et attaques possibles

- Les attaques en « force brute »

  Elles sont limitées dans le cas des disques durs, en effet le disque dur possède un compteur d'essai infructueux nécessitant le redémarrage du disque dur tous les 5 mots de passe erronés.

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Les contre-mesures et attaques possibles

- Suppression matérielle des sécurités

  Le changement de la carte mère d'un disque ne supprimera pas forcement le mot de passe de celui-ci (tout dépend du type de disque).

  Il existe aujourd'hui un marché prisé de vente de circuits électroniques de disques durs ou de composants.

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Conclusion

- La sécurité présentée au sein des disques durs est en grande partie liée aux méthodes de contournement conservée probablement pour des besoins industriels par les fabricants.

- La méconnaissance du milieu de la récupération de données et des outils d'analyse favorise se sentiment de « pseudo sécurité » même si l'affaire « XBOX » à mis en avant les limites de ce procédé.

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Recommandations

- Utiliser une disquette de 5’1/4 de qualité ;) ,

- ou un chiffrage total des données en temps réel pour le cache, l’OS, et les fichiers …

  un coût de 10 à 12% de CPU n’est pas forcement très élevé pour être réellement en sécurité.

  et on laisse l’authentification du disque dur en plus….

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Merci de votre attention

- Des questions ?
- Mon email sstic :

  sstic-ld@freesec.com
- Les recherches sur ce thème seront accessibles sur :

  Blog: www.pagesecurite.com

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net

Biographie

- http://www.acelab.ru/
- http://www.lecroy.com
- http://www.t13.org/
- http://hem.passagen.se/communication/ide.html

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.net