La protection d’accès des disques

Problématique

- Question : Comment protéger l’accès aux données d’un Macintosh® de manière simple et sûre ?
- Réponse : Dans l’absolu, l’installation d’un mécanisme de protection au niveau du driver du disque lui-même constitue la meilleure protection d’accès possible. Encore faut-il distinguer ce que l’on veut protéger, pour quel type d’utilisation, et savoir comment on le fait...

Contrôle d’accès au données se trouvant sur la machine

- Un mot de passe demandé au démarrage de la machine pour autoriser le montage d’un volume (qui peut être le disque tout entier) suffit le plus souvent. Mais ce mot de passe doit être incontournable.

La solution H-Drivor Protect : mot de passe “built in the driver” itself, avec ou sans encryption “à la volée”

H-Drivor est un ensemble d’utilitaires servant à assurer le formatage, le pilotage (via le driver), la configuration des disques durs, cartouches ou magnéto-optiques, et le montage automatique des supports éjectables, amovibles ou extractibles.

- Il intègre H-Drivor PROTECT, véritable application de configuration du driver qui permet d’installer en son sein différentes protections. L’installation du mécanisme de mot de passe dans le driver lui-même est la seule solution réellement fiable, car les drivers des périphériques SCSI sont les premiers chargés en mémoire à l’allumage de la machine,

immédiatement après les tests internes et... avant le système. Ce n’est qu’après chargement de tous les drivers SCSI des disques allumés que la machine pourra “booter” sur le disque et la partition de démarrage choisis.

- Le mot de passe de chaque volume protégé par H-Drivor Protect sera donc demandé dès l’allumage, soit avant même le “boot” sur le système, ce quels que soient la machine, le disque, le clavier ou le système ; cela permet de se prémunir contre une tentative de démarrage sur une disquette système ou l’installation invisible d’un débogueur dans le dossier système.

- Pour que la protection soit complète, H-Drivor Protect intègre également la possibilité de coder (encrypter) la ou les partitions protégées (et elles seules) ; une fois ce codage effectué, les données lues ou écrites sur le volume concerné seront décodées ou codées “à la volée” par le driver lui-même, sans aucune perte de temps par rapport aux lectures/écritures normales. Cela met à l’abri d’une tentative de récupération des données par l’installation sauvage d’un autre driver sur le disque, l’utilisation illicite d’un logiciel de récupération de données ou la tentative de relecture du disque secteur par secteur.
- Bien sûr, si un volume encodé est monté sur le bureau, ses fichiers pourront être copiés sous Finder sur n’importe quel support et relus ensuite en clair, puisqu’ils seront “décodés à la volée” par le driver au moment de la copie ; il s’agit là d’une utilisation normale d’un volume licitement monté. Glissez votre volume protégé à la corbeille avant d’aller boire un café…
- De la même façon, l’utilisation licite d’un récupérateur de données est possible ; il suffit pour cela de lancer H-Drivor Protect, de décoder le volume concerné et d’enlever son mot de passe, avant de lancer votre récupérateur préféré. Mais évidemment, ceci ne peut être fait que si l’utilisateur connaît le mot de passe… ou si l’administrateur lui-même intervient.
- Car H-Drivor Protect est également disponible, sur demande, avec une version “Administrateur” : une disquette spéciale permet alors à l’administrateur, en cas d’urgence (oubli du mot de passe par exemple), d’outrepasser — sans jamais les connaître — les mots de passe “utilisateurs”. Ce mécanisme, lié à la fois au mot de passe unique choisi par l’administrateur et à l’application propre au site, ne fonctionnera que sur le site

concerné.

Il va de soi que ce niveau de sécurité, cette simplicité et cette sûreté de fonctionnement impliquent que le disque à protéger soit formaté par H-Drivor, avant d'installer la protection de H-Drivor Protect.

Contrôle d'accès en environnement multi-utilisateurs

Peut être avez-vous besoin de permettre à plusieurs utilisateurs d'utiliser une même machine. Deux solutions s'offrent alors :

La solution H-Drivor Protect

- Il est possible de partitionner le ou les disques d'une machine en plusieurs volumes, chacun étant affecté à un utilisateur différent, qui y installera son propre mot de passe. Il suffira à l'utilisateur quittant le poste de travail, de démonter son volume en le glissant à la corbeille. et l'utilisateur suivant n'aura plus qu'à lancer H-Drivor Probe (ou H-Drivor Protect, ou H-Drivor Format) pour monter son propre volume en saisissant son mot de passe. Au démarrage, un utilisateur n'aura qu'à ignorer la demande de mot de passe des volumes qui ne lui appartiennent pas (en faisant trois fois "enter"), et il ne verra "monter" sur le bureau que le(s) volume(s) pour le(s)quel(s) il connaît le(s) mot(s) de passe.
- Il est également possible de réserver un lecteur de supports amovibles dans lequel chaque utilisateur insèrera son propre support, protégé par H-Drivor Protect. Il suffira à l'utilisateur quittant le poste de travail, de démonter son volume en le glissant à la corbeille, et à récupérer son support ; si le poste est muni de H-Drivor Probe ou H-Drivor Mount (version First), l'utilisateur suivant n'aura plus qu'à insérer son support qui montera automatiquement, non sans avoir demandé et reçu le mot de passe correspondant.

H-Drivor PRO (H-D Format, H-D Probe et H-D Protect) est fait pour cela.

La solution Cerbère (Prodiff)

- Cerbère sera utile, en revanche, dans le cas où vous devez gérer des postes multi-utilisateurs de type "libre-service". Cerbère permet en effet également :
  - de protéger l'accès au dossier système, en empêchant la modification des sous-dossiers Extensions et Tableaux de

bord,
- de protéger contre la copie illicite d'applications,
- de créer un dossier "individuel" par utilisateur, protégé par mot de passe,
- de créer des dossiers "de groupe" accessibles à plusieurs utilisateurs,
- d'autoriser l'utilisation de la machine par un "invité" (accès limité aux dossiers non protégés).

• Les changements d'utilisateurs en cours de session de travail se font simplement par une procédure de "delog/relog".
• L'installation de Cerbère se fait sur le driver Apple existant.

Développements possibles autour de H-Drivor Protect et Cerbère

De nouvelles versions de H-Drivor et de Cerbère sont en cours de préparation pour l'été. Elles intègreront de nombreuses fonctions nouvelles :

• Pour compléter le dispositif de sécurité au niveau du driver, Hédra offrira bientôt une protection d'accès à la machine par mot de passe et économiseur d'écran.
• Enfin, un lecteur de badge connecté au port ADB de la machine, et géré par le driver lui-même pourra apporter un niveau de protection supplémentaire ; ce système devrait être disponible en deux versions : lecteur pour badge magnétique et lecteur pour badge à infra-rouge sans contact, probablement avec un automatisme de mise sous protection automatique de la machine dès que l'utilisateur s'en éloigne un peu.

- Enfin, les mois qui viennent verront l’apparition de l’ensemble du concept de sécurité Hédra et de son intègration dans le nouveau système Apple…

Dans l’attente, nous serions heureux de recueillir vos impressions sur les produits actuels et les besoins d’évolution que vous pourriez ressentir, et sommes prêts à les étudier avec vous.