DECOUVERTE GAMECUBE

Soumis par robocop
02-08-2010

Le célèbre hacker TMBINC (l'inventeur du hack du BIOS de la Gamecube entre autres...) vient de trouver une particularité très intéressante. En étudiant avec un oscilloscope le disque original DATEL des codes triches pour Gamecube, il a découvert ce que l'on pourrait nommer "marque laser" qui n'est ni plus ni moins que la signature qui pemet d'authentifier le DVD pour la console.

L'image que vous voyez ci-dessus est la trace obtenue (voir le plat du signal):

Trace verte : Données HF provenant de la lentille laser.

Trace jaune : Horloge récupérée

Trace bleue : Données récupérées

En fait ce n'est pas une vraie marque laser physique mais la protection est incorporée dans le flux de données. Cette méthode est traditionnelle et n'est pas sans rappeller celle de la Dreamcast ou de la PS2. Pour ceux qui ne se souviennent plus DATEL avait décrypté cette série de données pour la PS2 et utilisé en fait la série d'un jeu original "Crazy Taxi" pour faire démarrer leur DVD.

Un hacker sur PS2 avait aussi trouvé la méthode sans vouloir la communiquer mais en donnant des débuts d'informations.Pour les hackers le jeu est d'essayer de reconstruire une image avec cette méthode. Cette découverte pourrait être un pas vers la fabrication de vrais "originaux"....mais il ne faut pas oublier que les deux pistes à explorer sont complexes.

La première solution est de refaire une image pour la graver. Or un graveur traditionnel ne sait pas reproduire toutes les informations et signaux de protections. Il faut donc modifier le firmware du graveur ou bien en deuxième solution la plus onéreuse : faire presser industriellement l'image en passant par une usine en créant un master avec un logiciel spécifique de mastérisation tout en restant discret...

Bon courage à ceux qui s'y mettront..

Source http://debugmo.de/2010/07/scope-pr0n/