HACK PS3 : Dump de l'hyperviseur (suite)

Soumis par robocop
14-02-2010

Toujours plongé dans le hack de la PS3, GeoHot a fait une déclaration plus qu'intéressante sur son blog. Avant de lire cette déclaration, il convient d'expliquer un peu l'architecture de la PS3: Le processeur de la PS3 se nomme le CELL, il se compose d'un processeur principal le PPE (PowerPc Processing Element) qui fait fonction de PPU (Physics Processing Unit) et de 8 coeurs spécifiques : les SPE (Synergistic Processing Elements) eux même dotés chacun d'une mémoire de stockage et d'un SPU (Streaming Processor Unit). Une petite explication s'impose sur les termes techniques suivants: "self" Exécutable au format .self (un peu comme les ELFPS2) "pkg" Exécutable au format .pkg (format du contenu téléchargé sur le PSN) "OtherOS" Exécutable nommé "otheros.bld", mode de lancement de Linux "Game OS" Le mode de fonctionnement natif des jeux. A ce jour la librairie du RSX qui gère la vidéo a été publiée et fonctionne en mode "Gameos". "Cell root key" Clef principale du processeur Cell "metldr" Partie du processus de démarrage La rom lance le metldr qui lance le lv0 qui lance le lv1ldr qui lance le lv1 "hyperviseur" En gros, une passerelle qui gère simultanément toutes les instructions de bas niveau ainsi que le système d’exploitation. Il sert aussi et surtout à vérifier l’intégrité du système.

Et maintenant que vous êtes un peu plus calé sur la PS3, voici la traduction du blog de Geohot Début de la traduction "Aujourd'hui j'ai vérifié mes théories sur le fait de faire tourner les SPUS isolées en tant que moteur de cryptage. Je crois que cela annule le dernier argument technique qui empêche la PS3 d'être hackée. Dans le mode "otherOS", toutes les 7 SPUs sont disponibles. Vous pouvez demander à une SPU (je vous laisse deviner laquelle je mets de côté) de charger le metldr, puis ensuite de charger le loader de votre choix et ensuite de décrypter ce que vous voulez, que ce soit des "pkgs" ou des "selfs". Et même pour des versions futures. Le PPU est situé plus haut dans la chaîne de contrôle que les SPU. Même si des vérifications sont ajoutées,(par exemple vérifier l'hyperviseur avant de décrypter le noyau), avec un système de mappage mémoire suffisamment malin vous pouvez cacher votre hyperviseur modifié. Ah, mais vous n'avez toujours pas la clef root du Cell. Et je ne l'aurais jamais et nous ne l'aurons jamais. Mais cela n'est pas utile. Par exemple nous n'avons pas non plus les clefs root de l'iPhone ou de la PSP. Mais je ne pense pas que quelqu'un doute du fait que ces systèmes soient hackés. Je me demande s'il y a encore des systèmes réellement sécurisés? " Fin de la traduction Geohot continue son avancée en utilisant un désassembleur pour lister le contenu de l'hyperviseur. En effet les docs des SPU sont publiées sur le net et Geohot a désormais un fichier binaire. Mais ce n'est pas le seule car CJPC du site http://www.ps3news.com/ a lui aussi réussi à dumper le contenu de l'hyperviseur PS3 et plus précisément le hyperviseur LV1 et le Bootloader LV0 à partir de la ram de la PS3. Ils ont utilisé le montage de Xorloser (voir news) en tapant comme des fous sur un bouton....Il s'est fait aider par un dénommé kakarotoks qui a réalisé un petit programme qui readirige la mémoire PS3 vers un endroit spécifique (un device /proc pour les linuxiens). Ce programme permets au noyau et à la zone utilisateur d'interagir. En gros le device /proc/ps3_hv_mem est créé lorsque le module kernel est inséré. Une fois fait on peut donc utiliser dd pour lire le device. En faisant ceci le device récupère les arguments pour les donner au programme lv1_peek qui à son tour lit la mémoire réelle. Attention! Il ne faut pas aller au delà de la mémoire supérieure de la PS3. Vers les 260Mo la PS3 a tendance à se planter, elle n'aime pas que l'on lise au delà des limites mémoire. En résumé il faut lancer l'exploit, le déclencher puis compiler le programme ps3_hv_mem.c ainsi qu'une version pré-compilée. Copiez les dans un dossier et compilez-les. Vous obtenez un module kernel ps3_hv_mem.ko ou bien utilisez la version pré-compilée. Tapez ensuite : sudo insmod ps3_hv_mem.ko Entrez le mot de passe et vérifier /proc pour voir si vous avez une entrée ps3_hv_mem ou bien grâce à la commande dmesg. Si c'est présent, on peut commencer. Vous pouvez dumper l'hyperviseur de la PS3 et le bootloader (ainsi que le reste de la mémoire réelle) avec la commande dd. Voici la syntaxe: dd if=/proc/ps3_hv_mem of=PS3_Memory_Dump.bin bs=1024 count=10K Cette ligne de commande dumpe 10485760 octets ou environ 10Mo ce qui inlcus le LV0 et le LV1. Finallement vous pouvez aussi augmenter la taille. D'après CJPC dans quelques temps l'hyperviseur sera cracké et probablement diffusé sur le net. La taille de l'hyperviseur ne sera pas un vrai souci car les 10Mo du dump se compressent en dessous de 2Mo. Si vous ne voulez pas vous embêter à effectuer le montage, il y a donc trois versions d'hyperviseur sur le net, celle de Geohot, de Xorloser et de CJPC. Ces versions sont propres à la machine et il est illégal de les télécharger et de les modifier. Bien sur le code de l'hyperviseur appartient à Sony mais une fois le reverse-engineering effectué on disposera d'un code entièrement réécrit ou alors il faudra trouver un bug et l'exploiter pour lancer une version modifiée. Concernant le code à proprement dit, Geohot confirme que les données peuvent être modifiées en ram avec la fonction lv1_poke et sauvegardée et donc la modification est permanente une fois faite. A ce jour on ne peut pas et on ne doit pas écrire n'importe ou en ram.. Geohot est en train de plancher sur le désassemblage de son hyperviseur en utilisant un langage à lui et des outils de reverse-engineering mais il est certain que le Hack PS3 avance à grand pas...