La première puce PS3

Soumis par robocop
08-02-2010

Traduction

Ce texte va tenter d'expliquer le matériel requis pour déclencher l'exploit d'accès à la mémoire de l'hyperviseur. Le but de ce matériel est d'empêcher la PS3 de sauvegarder un changement de valeur alors que ce n'est pas voulu du tout. La PS3 sauvegarde cette valeur en écrivant la valeur en mémoire. Cependant pour l'empêcher de sauvegarder la valeur modifiée nous devons stopper l'écriture en RAM. La PS3 envoies la commande d'écriture en RAM sur les lignes de contrôle. Donc nous devons interférer avec ces lignes de contrôle lorsque la commande d'écriture est envoyée.

Ce que nous voulons est faire croire à la PS3 qu'elle a réussi à écrire la valeur en RAM mais sans que la RAM reçoive la commande d'écriture. La manière la plus facile et plutôt sure d'interférer avec ces lignes de contrôle est de les mettre à la masse. Ceci peut être facilement en connectant un fil entre une ligne de contrôle et la masse. La partie la plus difficile est le "timing", il doit être juste pour que l'interaction ne se fasse qu'avec la commande d'écriture que l'on veut stopper et non pas avec tout ce qui peut arriver avant ou après cette écriture. Ceci peut être fait avec un équipement couteux et beaucoup de travail cependant Geohot a utilisé une méthode "chanceuse". Ceci implique de répéter continuellement pour avoir la chance d'écraser la commande d'écriture et de mettre en permanence à la masse une ligne de contrôle jusqu'à ce que soit quelque chose se plante alors que cela ne devrait pas ou que le but soit atteint en empêchant la commande d'écriture d'arriver.

A ce point l'exploit a donc été déclenché.

Maintenant que vous savez comment ça marche il est temps de l'implémenter. Une connexion est requise à la ligne de contrôle qui sera mise à la masse et une connexion à la masse. Ces deux fils ont besoin d'être connecté l'un à l'autre momentanément. Si vous voulez essayez et le faire manuellement aussi vite que vous pouvez pendant une milliseconde environ vous pouvez les connecter cependant les lignes de contrôle de la RAM sont très rapide et la durée de 1ms peut interférer avec trop de commandes. A la place ces lignes peuvent être connectées a un dispositif matériel capable de faire un pont entre pendant de brèves périodes de temps. Geohot suggère une période de connexion de 40 nanosecondes.

Il y a plusieurs façons pour qu'un dispositif matériel fasse cette courte connexion. Geohot utilise un FPGA qu'il avait sous la main pour le faire. D'autres préconisent d'utiliser un "timer" de type 555, mais je n'ai pas entendu que quelqu'un ait réussi avec ce montage.

J'ai utilisé un petit micro contrôleur sx28 que j'avais sous la main car j'en avais utilisé il y a quelques années pour un projet. Il fonctionne à 50MHz avec un cycle d'instruction de 20 microsecondes, ce qui signifie qu'il sera assez rapide pour fournir la connexion de 40 nanosecondes requise.

Le premier pas est de démonter la PS3 pour exposer le côté supérieur de la carte mère. Une fois ceci fait recherchez une des zones suivantes en fonction de la version de PS3 que vous avez. Cette première image provient d'une vieille PS3 60Go qui possède 4 ports USB et les lecteurs de cartes. Vous pouvez voir que j'ai soudé un fil sur le côté d'une résistance. Ceci a été fait pour la connexion vers la ligne de contrôle de la RAM de la PS3 que vous devez souder. Je vous suggère de faire passer ce fil vers le bas et puis vers la gauche du connecteur d'alimentation que vous pouvez apercevoir. Mon fil continue vers le bas sur cette photo mais j'ai trouvé qu'en faisant ainsi cela causait des interférences dans le fil ce qui déclencherais de façon non voulue des corruptions de la RAM. Pour éviter ceci vous devez router le fil vers la gauche en dessous du connecteur d'alimentation pour qu'il puisse ressortir sur le côté gauche du boitier de la PS3. Vous pouvez utiliser un long fil durant l'installation, mais lorsque vous finaliserez l'installation essayez de le garder aussi court que possible. Vous pouvez voir que j'ai utilisé de la colle pour éviter qu'il y ait des tensions sur le fil qui puissent décoller la soudure.

Cette seconde image provient d'une PS3 80Go avec 2 ports USB et aucun lecteur de carte. C'est le modèle sorti avant que la grosse PS3 soit remplacée par la PS3 "slim", il s'agit donc d'une nouvelle révision de carte mère ou se trouvent deux puces pour la RAM de chaque côté de la carte mère au lieu de trouver tous les 4 du même côté. Sur cette photo j'ai entouré la trace ou vous devez souder la connexion sur les lignes de contrôle. Pour souder celle-ci j'ai utilisé un scalpel pour égratigner soigneusement la peinture pour exposer le suivre en dessous et ensuite y souder un fil. Une fois connecté vous devez router ce fil tour droit vers le devant du boitier de la console pour éviter les interférences avec les autres parties de la PS3. Une fois encore essayez de garder le fil le plus court possible.

Ensuite vous devez obtenir une connexion à la masse. Il s'agit de la même méthode pour les deux versions de cartes mère et très facile à faire. Vous pouvez juste enrouler un fil autour de n'importe laquelle des vis métalliques qui se fixent dans le couvercle en métal qui couvre la carte mère. Vous n'avez même pas besoin de souder, entourez le fil autour de la tête et revissez la en place :) Ce fil doit être sorti de la console en même temps et à côté de l'autre fil de contrôle.

Les deux connexions filaires sont communes à toute implémentation du déclenchement matériel de la faille. Ce qui suit est spécifique à la façon dont je déclenche la faille mais vous pouvez en faire de même. J'avais essaye initialement de souder un fil pour prendre le 5 volts de l'alimentation mais cela a créé des interférences dans les lignes de contrôle ce qui faisait planter la PS3 au démarrage.

Pour mon déclenchement matériel j'ai utilisé un micro contrôleur SX28 que j'avais acheté il y a des années et qui faisait partie d'un kit de programmation. Pour utiliser le SX28, il vous faut un SX28, une façon de le programmer(SX-Key ou SX-Blitz) et un quartz pour gérer le SX 28 à 50MHz. Tout ceci est bien sur inclus dans les kit mentionnés ci-dessus. Peut être que si suffisamment de gens achètent leurs kits et mentionnent mon pseudo xorloser ils m'enverront une version USB du SX-Key au lieu de mon vieux kit basé sur un port série :/

Ci-dessous est un schéma approximatif de mon circuit que j'ai dessiné avec windows paint. Notez bien que j'utilise le kit de programmation que j'ai mentionné ci-dessus qui utilise le programmateur SX-Key à la place d'un oscillateur quand le SX-Key est connecté. Je n'ai pas d'oscillateur externe donc je vous laisse faire le reste. Doc notez bien que vous devez avoir soit un quartz OU un SX-Key connecté pour que la puce tourne.

Ce code source pour le SX28 est la dernière pièce du puzzle. Programmez votre SX28 en utilisant le logiciel gratuit "SX-Key Editor" de chez Parallax. Une fois ceci fait et connecté à la PS3 vous devez être capable d'envoyer une "impulsion" (mise à la terre de la ligne de contrôle) à la PS3 en appuyant sur l'interrupteur. Vous devez utiliser un bouton à contact temporaire pour cela car il continue d'envoyer des impulsions toute les les 100ms si l'interrupteur reste connecté. La DEL sur le côté droit du schéma est juste la pour donner un retour à l'opérateur. Elle s'allume lorsqu'une impulsion est envoyée pour vous permettre de savoir si le circuit fonctionne correctement comme il le doit. Il devrait mentionner que si vous regardez mon code pour le SX28 vous verrez qu'on pourrait croire que j'envoie une impulsion longue de 360 nanosecondes. Je ne sais pas la durée de l'impulsion réellement envoyée car je n'ai (encore) aucun matériel pour mesurer l'impulsion.

Il y a probablement des délais induits qui arrivent lorsque l'on change la direction du port ce qui signifie que bien que j'attende 360 ns, il envoie toujours une impulsion de 40 ns environ. Pour arriver à la valeur de 360 ns j'ai essayé plusieurs valeurs en raccourcissant la valeur autant que possible jusqu'à ce que je ne déclenche plus la faille, puis j'ai augmenté un tout petit peu pour obtenir la valeur la plus courte qui fonctionne encore.

Ouf, enfin la fin de ce texte. Mon prochain texte portera sur du lgoiciel que j'ai écrit pour réaliser une copie de votre propre superviseur et plus...

Fin de la traduction

La puce PS3 ou un hack logiciel?

Bien sur vous l'avez compris en lisant ce texte, tout est basé sur la faille. Cette faille permettra sans doute de passer outre les protections de l'hyperviseur et donc aujourd'hui nul ne peux dire si la puce sera indispensable de façon permanente ou non. Nul ne sait nom plus quand sera disponible un chargeur de backups pour la PS3 mais à mon humble avis c'est pour cette année.

Le matériel

Ne vous précipitez pas de suite sur le net pour acheter un programmateur SX KEY et SX Blitz sauf si vous êtes curieux mais surtout car il existe des tas de façons en électronique pour générer une impulsion de 40ns. De plus ces kits ne sont pas très répandus. Patientez encore un peu et les prochains montages seront moins onéreux que celui-ci. Il est même possible par exemple de réutiliser une puce existante pour cela en changeant son firmware.

De plus certains sont même à la recherche de cette impulsion directement sur la carte mère de la PS3! Dans ce cas le matériel a installer et le coût serait réduit. Les poseurs de puce seront heureux aussi de voir que le nombre de fils est réduit et la soudure à la portée de tout un chacun possédant de bonnes connaissances en soudure.

Le logiciel

Aucun logiciel développé pour l'instant mais dès que le logiciel permettant de dumper l'hyperviseur sera disponible ce

ne sera plus qu'une question de quelques mois avant que ne soit disponible un programme permettant de lire ses propres backups. Et l'avenir?

Une fois la partie logicielle dévoilée on passera par les étapes classiques de fabrication des puces. Si l'on se base sur les puces des autres consoles on peut distinguer plusieurs étapes.

Phase 0 : La puce faite maison

Phase 1 : La puce de première génération

Phase 2 : La deuxième génération avec mise à jour par DVD

Phase 3 : La puce sans soudure ou clipsable

Phase 4 : La puce de quatrième génération avec gestion de disque dur

Mais ceci est une autre histoire...nous en sommes à peine à la phase 0...