La fin de Grsecurity ?

Posté par patrick_g (page perso) le 06/01/09 à 16:54. Modéré par Nÿco.
Tags : grsecurity

Grsecurity est un patch sous licence GPL pour Linux qui vise a renforcer la sécurité du noyau par l'ajout de divers mécanismes.

Le sponsor principal du projet s'étant retiré du fait de la crise économique, la version 2.1.12 de Grsecurity pourrait bien être la dernière. Selon l'annonce postée sur le site, si un nouveau sponsor ne se manifeste pas avant le 31 mars alors les développements prendront fin et le projet sera gelé, peut-être définitivement.

- Le projet Grsecurity (131 clics)
- L'annonce de la dernière version (47 clics)
- Comment utiliser Grsecurity (pdf) (89 clics)
- L'avis de Linus Torvalds (166 clics)

Grsecurity propose une multitude de fonctions pour renforcer la sécurité de Linux et pour contrer les diverses attaques qui visent à prendre le contrôle du noyau.
En premier lieu Grsecurity inclut le patch PaX qui permet de rendre aléatoire les adresses mémoires et d'empêcher l'écriture sur les portions mémoires contenant du code exécutable.
Grsecurity permet également de renforcer la résistance du mécanisme de Chroot (qui sert à isoler un programme dans un système de fichier afin de le sécuriser).
Des fonctions d'audit sont ajoutées dans le noyau afin de mieux surveiller ce qui se passe sur une machine et d'être averti plus vite en cas d'attaque.
La fonction Trusted Path permet d'interdire l'exécution des binaires dont le propriétaire n'est pas administrateur.

En ce qui concerne les restrictions d'accès Grsecurity utilise un modèle de sécurité à base de rôles (RBAC) alors que le modèle de sécurité de SELinux est plutôt celui du contrôle d'accès obligatoire (MAC). Cette différence de philosophie est aggravée par le refus des développeurs de Grsecurity d'utiliser LSM.
En effet, afin d'éviter d'avoir à choisir entre différents modules de sécurité et compte tenu du fait que les développeurs s'écharpaient sur les listes de diffusion, Linus a décidé de privilégier une infrastructure unique sur laquelle viendraient de greffer les modules concurrents.
Cette infrastructure LSM (Linux Security Modules) est utilisé par les modules SELinux et SMACK mais Grsecurity a toujours refusé de jouer le jeu.
Selon les développeurs du projet ce serait une erreur que d'utiliser LSM car cette infrastructure souffrirait de problèmes techniques. Tout d'abord les crochets (hooks) permettant à l'infrastructure de présenter des points d'entrée aux différents modules seraient mal pensés. En nombre insuffisant et spécialisés dans une architecture de contrôle d'accès qui n'est pas celle de Grsecurity, ces hooks ne sont pas adaptés au projet et sont mêmes accusés de faciliter le travail de rootkit pour s'implanter dans le noyau.
Cette critique radicale de LSM est disponible sur le site du projet et on peut y lire entre les lignes qu'il existe une certaine rancœur envers SELinux qui est perçu comme ayant une volonté hégémonique.

À cause de ce refus de l'infrastructure LSM, le patch Grsecurity/PaX n'a jamais pu entrer dans le noyau Linux ce qui a eu de lourdes conséquences. En effet, n'étant jamais entré dans la branche principale, le patch Grsecurity doit être maintenu et adapté par les développeurs du projet afin de rester compatible avec un noyau Linux qui bouge très vite. Ce travail supplémentaire explique le fait que les versions de Grsecurity ne sont pas compatibles avec toutes les versions du noyau. Il y a des « trous » dans la disponibilité du patch puisque, par exemple, la version 2.1.11 est prévue pour les noyau 2.6.24.x alors que la version 2.1.12 est adapté au noyau 2.6.27.x.
Si par malchance vous utilisez un noyau 2.6.25 ou 2.6.26 alors vous ne pourrez pas profiter de Grsecurity (sauf rétroportage effectué par votre distribution).

Un problème plus subtil est celui de la reconnaissance par les sponsors éventuels. Comment faire valoir son excellence technique et obtenir des subsides si on n'arrive pas à intégrer le noyau Linux officiel ? Il est probable que de nombreux sponsors et contributeurs potentiels ont été et continuent à être rebutés par cette absence de perspective d'intégration.
Ce problème est d'ailleurs bien perçu par les partisans de Grsecurity et de PaX qui, après l'annonce des difficultés du projet, ont effectuée une nouvelle tentative en vue d'une entrée dans la branche principale. Ce post sur la liste de diffusion de Linux pose clairement la question: « *Avant que le projet ne meure je voudrais attirer encore une fois votre attention sur la question de l'intégration dans le noyau* ».
La réponse de Linus a été fort peu encourageante :
« Franchement ces patchs ont toujours été un mélange de :
- trucs raisonnables
- code invasif complètement stupide
Un exemple de la deuxième catégorie est le patch totalement idiot d'émulation pourrie du bit NX. Cette sorte de patch ajoute simplement de la saleté non maintenable et n'est même pas utile sur le long terme. N'importe quel mainteneur sain d'esprit (moi) devrait refuser son intégration.
L'apparente inaptitude (et, plus important encore, le manque total de volonté) de la part de l'équipe PaX pour comprendre ce qui doit ou pas être intégré dans un noyau, de découper leur code et de tenter d'intégrer les parties de bonne qualité (et de savoir reconnaitre les parties pourries ou trop spécialisées pour entrer dans le noyau) a conduit à la non intégration des fonctions de PaX.
Non je ne vais pas soudainement commencer à accepter ce code juste parce que le projet est en mauvaise posture. Aucun des problèmes de base n'a été résolu ».

À suivre les échanges sur la liste de diffusion il semble clair que les partisans de Grsecurity n'ont pas bien compris le modèle de développement du noyau Linux et ce ne sont pas leurs appels pour sauver le projet qui vont y changer quoi que ce soit.
Robert Hancock a détaillé pour eux la marche a suivre :
« Tout ça c'est bien joli mais ce ne sont pas des messages qui vont faire avancer les choses. Si ces gens veulent inclure leur code dans la branche principale alors le chemin est le même que pour tous les autres : proposer des patchs concrets, qui améliorent pas à pas le fonctionnement et qui ne font pas doublon avec des fonctions déjà présentes. Des patchs qui relèvent clairement du noyau et pas de l'espace utilisateur, qui n'ajoutent pas une charge de maintenance inacceptable, etc.
Si de tels patchs sont soumis alors ils auront le potentiel pour être acceptés. La question est : pourquoi les gars de Grsecurity n'ont pas fait ça avant par opposition à maintenant qu'ils sont en crise ?
Dire aux développeurs de Linux "Hé, incluez ce gros bout de code dans votre noyau sinon on reprend notre joujou et on rentre chez nous" n'est pas la bonne méthode ».

Les perspectives d'inclusion étant donc sombres, il semble peu probable que Grsecurity/PaX survive à cette crise sans l'apparition d'un sponsor décidé à faire vivre le projet. Grsecurity se bat pour sa survie et fait la publicité de ses fonctions afin de démonter que ses choix étaient bons depuis des années. Un graphique illustrant l'influence du projet sur les autres systèmes d'exploitation a été créé et est accessible sur le site.

Il serait dommage que ce projet, jouant souvent le rôle d'aiguillon et de défricheur, ne soit plus en mesure d'avancer et disparaisse définitivement.

Difficulté d'être inclu dans le noyau

Posté par Victor STINNER (page perso) le 06/01/09 à 17:45. Évalué à 10.

Le patch grsecurity modifie 539 files fichiers et fait environ 37.000 lignes. C'est un très gros patch monolithique qui doit être redécoupé pour être inclu dans le noyau. Est-ce que ce travail a déjà été fait ?

PaX seul modifie 455 fichiers et pèse environ 23.000 lignes.

Re: Difficulté d'être inclu dans le noyau

Posté par Amaury le 06/01/09 à 18:11. Évalué à 3.

Grosso modo GRsecurity se prend dans la figure exactement ce que Greg Kroah Hartman avait décrit [1] lors d'une conférence en Juin 2008 (je paraphrase) :
"*compte tenu de la complexité et de la vitesse d'évolution du kernel, il est de plus en plus difficile de maintenir un patch* ***en dehors*** *de l'organisation, la solution la plus efficace consiste à inclure ses patches dans la branche officielle du noyau.*".

[1] http://www.youtube.com/watch?v=L2SED6sewRw

Re: Difficulté d'être inclu dans le noyau

Posté par Pierre Jarillon (page perso) le 07/01/09 à 14:13. Évalué à 10.

Le gros mérite de Linus Torvalds, c'est d'avoir su gérer le premier gros projet sur Internet. Ce projet aura 18 ans cette année et je pense que Linus a maintenant une sacrée expérience.

L'expérience m'a montré qu'avec le temps un logiciel pouvait soit se parfaire soit se cochonner. C'est ce qui arrive régulièrement lorsqu'une entreprise fait appel à la sous-traitance pour faire des travaux avec des contraintes de délai. Le danger est d'inclure des verrues qui nécessitent par la suite d'autres verrues et ainsi de suite. C'est ainsi que l'on peut pourrir un code source. Lorsque le code est ouvert, on s'aperçoit de tout ce qu'il faut réécrire (je pense à Netscape).

Conserver un code propre est un impératif et on ne peut pas reprocher à Linus de l'avoir négligé.

Re: Difficulté d'être inclu dans le noyau

Posté par patrick_g (page perso) le 06/01/09 à 18:11. Évalué à 7.

>>> C'est un très gros patch monolithique qui doit être redécoupé pour être inclu dans le noyau. Est-ce que ce travail a déjà été fait ?

je ne crois pas.
Je suis très pessimiste sur une quelconque inclusion dans le noyau car les devs de PaX et Grsecurity ne semblent absolument pas prêts à bosser en suivant les règles de dev Linux.
Il y a beaucoup d'acrimonie dans les messages et j'ai même vu des échanges assez trollesques sur LWN initié par Brad Spender (de Grsecurity) et par un user PaXTeam.
Exemple ici : http://lwn.net/Articles/286263/

C'est dommage car ces mecs sont visiblement très compétents....mais il faut aussi avoir l'humilité d'accepter certaines contraintes quand on veut que son code soit mergé dans un projet géré par d'autres personnes.

Re: Difficulté d'être inclu dans le noyau

Posté par bilboa le 06/01/09 à 18:30. Évalué à 6.

le vrai problème, c'est que ce sont des patchs visant a avoir un niveau de sécurité maximum.
en acceptant les "contraintes" ou plutôt les choix de Linus/Linux/LSM/Communauté/etc ca veut dire que le niveau de sécurité serait plus bas.

C'est ca, le vrai problème pour grsec/pax

Re: Difficulté d'être inclu dans le noyau

Posté par Victor STINNER (page perso) le 06/01/09 à 20:40. Évalué à 10.

Si 80% des patchs de Grsecurity étaient intégrés upstream, je pense que la maintenance de Grsecurity serait déjà plus simple. On pourrait même penser qu'il y aurait plus d'utilisateurs. Si le code est dans le noyau, ça donne confiance, ex: quand à la pérénité.... Les 20% restant seraient maintenus en dehors et serviraient à renforcer encore la sécurité.

Le « problème » est qu'il faut être patient, faire de petits patchs, accepter les critiques, et suivre les règles :-) Ça me rappelle le dernier ordonnanceur de processus : y'avait deux projets en lice et celui qui a gagné n'était pas le meilleur, mais celui qui a accepté les critiques.

Re: Difficulté d'être inclu dans le noyau

Posté par fweisbec le 06/01/09 à 20:43. Évalué à 2.

Y'avait un autre ordonnanceur contre CFS?

Re: Difficulté d'être inclu dans le noyau

Posté par Spack le 06/01/09 à 21:36. Évalué à 10.

> Y'avait un autre ordonnanceur contre CFS?

Il s'agit de Staircase Deadline (SD) de Con Kolivas ce qui entraîna d'ailleurs l'arrêt de ses contributions au noyau...

http://kerneltrap.org/node/14008

Re: Difficulté d'être inclu dans le noyau

Posté par naurel le 06/01/09 à 23:39. Évalué à 9.

les positions de "grand dictateur" de linus ont l'avantage de faire avancer le projet mais l'inconvénent de faire degager ceux qui ne sont pas d'accord, même s'ils proposent des améliorations significatives que de nombreuses personnes auraient aimé voire il y a très longtemps !

De plus les positions de torvalds envers la sécurité sont vraiment très moyennes, on passe en douce des grosses corrections de trous de secu ...
En espérant que tout le monde mette son noyau a jour tranquillement sans s'en apercevoir, sans jamais mettre le CVE dans le changelog du patch, avec un commentaire obscur... charge aux distributions linux ensuite de retrouver leurs petits pour proposer des mises a jour de sécurité ...
D'ailleurs il faut voir que par exemple gentoo a complètement abandonné de faire des mises a jour de sécurité ou des annonces de vulnérabilité depuis des années pour le noyau.

Re: Difficulté d'être inclu dans le noyau

Posté par IsNotGood le 07/01/09 à 02:10. Évalué à 5.

Ça me fait rigoler tous ces critiques de circonstance envers le développement de Linux. Les développeurs de Grsecurity sont géniaux, malheureusement incompris par cet abrutis de Linus et les développeurs Linux. Ben voyons...

Oui Linus Torvals fait des conneris. Il en dit aussi. Mais la rapport bonnes décisions sur mauvaises est excellent.

> mais l'inconvénent de faire degager ceux qui ne sont pas d'accord

Et l'avantage de ne pas avoir Linux codé avec les pieds avec des fausses idées réellement bancales.

> même s'ils proposent des améliorations significatives que de nombreuses personnes auraient aimé voire il y a très longtemps !

Aujourd'hui il y a SMACK et SeLinux dans Linux. Il y aura peut-être AppArmor (vers 2.6.30 ?). Dans ces trois il y a une controverse avec AppArmor, m'enfin, il sera peut-être là. Ici on reproche à Linus de ne pas faire de place à Grsecurité car il serait "buté", mais il y a déjà 3 systèmes de sécurité dans Linux ! Linus a voulu de LSM ! Quelle ouverture !
Et l'ouverture de Grsecurity ? Ben c'est : "non merci".

Linus était-il vraiment ouvert pour les questions de sécurité ? Pas vraiment car ça ne l'intéresse pas et ne s'en cache pas. À tord ou à raison il n'a pas voulu choisir entre SMACK ou SeLinux ou AppArmor ou autre.
Ici on reproche à Linux d'être "difficile d'accès" pour un développeur alors que c'est l'ouverture de Linux qui fait qu'il est difficile pour un projet de vivre hors de team Linus Torvalds.

La problème de Grsecurity n'est pas qu'il était trop "sûr", mais que techniquement il y avait nombres de choses qui ne plaisaient pas à Linus (et pas seulement lui), que les développeurs de Grsecurity refusaient les critiques (Linus a horreur de ça => voir Con Kolivas), que Grsecurity n'a rien fait pour répondre aux exigences, qui ont fait leur preuve, de Linux.

> des améliorations significatives que de nombreuses personnes auraient aimé voire il y a très longtemps !

Es-ce qu'on est mal servi avec SeLinux ?
En passant, Nx a aussi été développé par Red Hat pour i386. Comme pour Pax, il n'a pas été accèpté. Red Hat n'a pas chié une pendule.

> sans jamais mettre le CVE

Tu trouveras certaines distributions qui le font. En fait, c'est moins les développeurs qui suivent les CVE que des équipes dédiées à la sécurité.
Enfin, il y a une période d'ambargo (le temps que les distributions soient prête). C'est seulement du bon sens.

Re: Difficulté d'être inclu dans le noyau

Posté par feth (page perso) le 07/01/09 à 18:23. Évalué à 5.

Je suis d'accord avec ce que je parviens à déchiffrer de ton commentaire, mais j'ai les yeux qui saignent, là.

Re: Difficulté d'être inclu dans le noyau

Posté par briaeros007 le 07/01/09 à 16:43. Évalué à 4.

des grosses corrections de trous de secu ...
L'intérêt que je vois est d'essayer d'éviter que les script kiddies puisse utiliser ces changelogs à mauvais escient.
Alors certe ce n'est pas de la sécurité, mais si ca permet d'éviter 99% des attaques "idiotes" (il y a forcément un délai entre le moment de la mise à jour du noyau, et le moment ou tu vas relancer ta machine. Surtout sur des machines des prods!)

Ensuite si ça ce trouve, c'est juste de la flemme :P

Re: Difficulté d'être inclu dans le noyau

Posté par patrick_g (page perso) le 07/01/09 à 17:36. Évalué à 10.

>>> Ensuite si ça ce trouve, c'est juste de la flemme :P

D'après ce que j'ai lu sur LWN le problème c'est que si on indique qu'une correction bouche un trou de sécu cela implique que les autres corrections ne concernent pas la sécurité.
Hors il est très, très difficile (presque impossible) de savoir si un bug a ou pas des implications sur la sécurité du système.
La solution retenu par GKH (qui manage la branche 2.6.x.y) c'est de ne pas s'embêter a essayer de faire la différence entre les corrections de trou de sécu et les autres. Un user doit appliquer les correctifs, tous les correctifs, et ne pas tenter de jouer au plus fin en sélectionnant les corrections.

Re: Difficulté d'être inclu dans le noyau

Posté par Victor STINNER (page perso) le 08/01/09 à 03:01. Évalué à 2.

D'après ce que j'ai lu sur LWN le problème c'est que si on indique qu'une correction bouche un trou de sécu cela implique que les autres corrections ne concernent pas la sécurité.

Euh non, pas nécessairement. Marquer qu'un commit corrige une vulnérabilité n'indique rien quant aux autres commits. Ça demande aussi un peu de bon sens : la majorité des développeurs sont incapables de savoir si un bug quelconque peut avoir une implication sur la sécurité. Je préfère largement que les failles connues soient explicitement notées.

Re: Difficulté d'être inclu dans le noyau

Posté par patrick_g (page perso) le 08/01/09 à 08:28. Évalué à 3.

>>> Marquer qu'un commit corrige une vulnérabilité n'indique rien quant aux autres commits.

Pour toi et moi OK. Mais visiblement il y a pas mal de gens qui considèrent que si un correctif n'est pas marqué comme étant lié à un problème de sécurité alors c'est qu'il n'a aucune implication quand à la sécurité du système.
C'est évidemment faux et, pour combattre ce sentiment, GKH a décidé d'éviter de s'emmerder à décrire toutes les implications possibles et imaginables des bugs détectés.

Re: Difficulté d'être inclu dans le noyau

Posté par Littleboy le 08/01/09 à 11:06. Évalué à 6.

Ouais, enfin le probleme ce n'est pas de ne pas chercher et decrire des possibles problemes de secu, c'est de les cacher de facon volontaire.

Et c'est justement ce qu'il est reproche a Linus et a d'autres developpeurs du noyau: de ne pas noter les infos quand le probleme a ete etudie et leur a ete transmis (ie une faille exploitable, avec historique du probleme et les personnes par qui c'est passe, eventuellement un numero CVE qui devient un commit avec un commentaire de 1 ligne). Et franchement quand on voit certains commits, c'est limite du foutage de gueule.

Oh, un joli buffer-overflow (apparemment exploitable) avec comme description du commit "eviter de copier des chaines de caracteres trop longues" :D

Meme si Brad est un gros trolleur et souvent de tres mauvaise foi, ca fait peur quand meme. Et cette secu par l'obscurite (sur les commentaires de correction de bug...), ca pue vraiment beaucoup. Ca n'empeche pas les gens qui cherchent des vulnerabilite a exploiter de le faire, ca emmerde juste les developpeurs et integrateurs en cachant des informations importantes. Autant utiliser windows a ce moment la, au moins la secu par l'obscurite marche vraiment (un peu) dans ce cas la...

Re: Difficulté d'être inclu dans le noyau

Posté par briaeros007 le 06/01/09 à 23:04. Évalué à 6.

ce n'est pas pour une raison de sécurité que les patchs ne sont pas accepté, mais (au vu de la dépeche en tout cas) parce qu'ils ne respectent les différentes séparation kernel/userspace/... (séparation qui selon toute logique devrait AUGMENTER la sécurité).

Bref, si tu as des arguments autres que juste "le modèle de dvp de linux ne permet pas le niveau de sécurité maximum qu'offre grsecurity", je suis preneur, mais tant que ces arguments apparraissent pas, je reste fortement dubitatif.

Re: Difficulté d'être inclu dans le noyau

Posté par bilboa le 08/01/09 à 14:00. Évalué à 1.

non, le problème c'est que grsecurity refuse d'utiliser LSM.

Oui, LSM est un problème. Non, ce n'est pas la fin du monde.
Oui, SELinux voulais virer LSM pour de bonne raisons.
Oui, SELinux voulais LSM a la base, pour des raisons politiques.
Oui, virer LSM maintenant que SELinux est implementé est aussi pour raison politiques (mais aussi techniques, donc).
Oui, c'est pour ca que SMACK à été intégré (linus s'est pas laissé berné quoi)

Le reste n'étant pas de design de base, c'est du patch a corriger etc pour être correct/conforme au noyau.

Les arguments contre LSM sont nombres, suffit d'aller sur le site de grsecurity ou rsbac pour lire les arguments (ils ont des pages spéciales a ce sujet)

Re: Difficulté d'être inclu dans le noyau

Posté par briaeros007 le 08/01/09 à 14:43. Évalué à 5.

j'ai lu les commentaires sur LSM sur le site de grsecurity, et il me fait un peu penser à certains partis d'opposition en france .
Je vais citer les grands "titres" :

Why grsecurity cannot use LSM
Why LSM will harm the security of all Linux systems
Why I personally dislike LSM

Alors tout ce que je vois c'est des commentaires indiquant que "ouais LSM c'est pas bien".
Les commentaires sont certainement pertinent (même si j'ai un doute sur un ou deux), mais je ne vois pas de proposition de sa part.
Par exemple un moment il dis "LSM c'est juste du contrôle d'accès, grsecurity a besoin de plein d'autres choses. On devra quand même patcher le noyau".
Ben PROPOSE une modification de LSM qui conviendra a tes besoins et qui sera assez générique pour que tous les autres puisse la vouloir. (C'est du boulot, j'en suis bien conscient).
(C'est aussi ça la politique, faire des concessions : ok je veux bien faire des efforts pour accepter vos trucs, alors est ce que vous pouvez accepter ça).
Si le patch grsecurity est si bien et que son mode de fonctionnement est bien pensé, cela ne devrais pas poser trop de problème de proposer des "hooks" différents à LSM ?

ou encore *The amount of work I spend porting to new kernel releases is minimal.*
pourtant en lisant la dépêche , moi je vois ça
Il y a des « trous » dans la disponibilité du patch puisque, par exemple, la version 2.1.11 est prévue pour les noyau 2.6.24.x alors que la version 2.1.12 est adapté au noyau 2.6.27.x.
Si par malchance vous utilisez un noyau 2.6.25 ou 2.6.26 alors vous ne pourrez pas profiter de Grsecurity (sauf rétroportage effectué par votre distribution).

Visiblement ce n'est pas si minimal que ça.

Comprend moi bien, je ne dis pas que "grsecurity y font que raler, ils ont que ce qu'ils méritent", mais "c'est facile de dire que c'est toujours de la faute des autres, mais les torts sont à 99% du temps partagés!"

Re: Difficulté d'être inclu dans le noyau

Posté par patrick_g (page perso) le 08/01/09 à 16:26. Évalué à 7.

Surtout que les modifs sur LSM c'est possible.
Dans le futur 2.6.29 y'a des nouveaux hooks qui ont été ajoutés à LSM pour pouvoir faire des modules de sécurité basés sur le chemin d'accès (pathname) comme TOMOYO ou AppArmor.
Donc ce serait parfaitement possible aux gars de Grsecurity de proposer des hooks adaptés à leurs besoins (si leurs besoins sont jugés solides par les devs Linux).

Re: Difficulté d'être inclu dans le noyau

Posté par xhub le 08/01/09 à 22:34. Évalué à 2.

<disclaimer>Je suis un utlisateur de GrSEc/PaX </disclaimer>

Oui mais un des problème est que les gens qui jugent ceci n'ont peut être pas la sécurité comme une de leurs priorité. Pour prendre l'exemple de Linus déjà cité ici, il possède beaucoup de qualités, mais je n'ai pas l'impression qu'il accorde une place si importante que ça à la sécurité.
Plus il y a fort à parier que les gens qui sont derrière les autres modèles de sécurités bouchent un peu le passage.
Mais à mon avis la direction prise par le projet GrSec/Pax est déjà fondamentalement la bonne : proposer un modèle qui travaille en l'amount, pas en aval comme SeLinux(et d'autres peut être), qui de manière un peu fallacieuse peut être considérer comme un modèle qui joue le rôle de rustine.
Je me permet ici de rappeler que lors du dernier grand coup d'éclat en manière de sécurité niveau kernel (lire le local root exploit de février 2008), GrSec/PaX permettait de s'en prémunir : on était juste exposé à une attaque de type DoS car chaque exécution de l'exploit "salissait" un petit bout de mémoire. Il ne me semble pas que les autres modèles permettaient une telle protection (mais je peux me tromper).

Re: Difficulté d'être inclu dans le noyau

Posté par briaeros007 le 08/01/09 à 22:56. Évalué à 7.

et je suis persuadé que apparmor arrive* a "contrer" des attaques que selinux n'arrive pas, et que selinux arrive* à "contrer" des attaques que grsecurity n'arrive pas.

*Avec un temps fini et sensiblement équivalent pour configurer tout le bousin.

Qu'un exemple montre que dans ce cas précis grsxecurity saisbien, prouve que grsecurity peut etre utile, mais ne donne aucune indication sur la pertinence des autres solutions.

Le prix du développement out-of-tree

Posté par fweisbec le 06/01/09 à 18:20. Évalué à 10.

C'est le prix à payer lorsqu'on développe un projet pour le noyau sans travailler avec le reste de la communauté. Certes peut être qu'ils n'acceptaient pas de bosser sur une base bancale. Alors en ce cas il fallait envoyer des patchs pour virer ces mauvaises bases et les tourner petit à petit vers ce qu'ils voulaient tout en apportant régulièrement l'argumentation qui va avec.

C'est déjà parfois difficile de faire avaler aux mainteneurs un petit jeu de 10 petits patchs qui développe une idée travaillée de manière isolée sans en parler à la communauté. A moins d'avoir de la chance ou beaucoup d'expérience.
En règle générale, soit l'idée est carrément refusée, soit on applique les révisions des rélecteurs de patchs et on renvoie une nouvelle version de son jeu de patch, et on itère comme ça jusqu'à ce que ça plaise à tout le monde. On voit régulièrement passer, sur la mailing list de Linux, des patchs qui en sont à leur 5ème, 10 ème version.
Enfin heureusement ce n'est pas toujours comme ça. Au delà de 5 itérations c'est quand même plus rare. Mais ça peut être comme ça au lancement d'un projet pour le kernel et après la suite du développement est souvent plus simple et plus fluide, une fois qu'on a compris comment accorder ses propres désirs avec la direction que veut prendre la communauté, on parvient à balancer des patchs qui sont inclus sans trop de besoin de correction.

Bref, je parlais là d'un petit jeu de 10 petits patchs. Mais leur truc est un pavé.

C'est difficile d'inclure un pavé dans le noyau, l'idéal étant d'inclure chaque fonctionnalité d'un projet petit à petit, en restant toujours très proche de la liste de diffusion.
Si un changement nécessite d'un coup un gros patch, il faut toujours parler de son idée avant et voir l'avis des autres, au risque d'être frustré après avoir balancé un patch de plusieurs semaines de boulot sans en en avoir parlé avant.

Chantage

Posté par Aris Adamantiadis (page perso) le 06/01/09 à 19:27. Évalué à 10.

Le chantage à l'abandon du support de grsec, brad nous l'a déjà fait il y a 2 ans quand il avait besoin grave de thunes. Evidement que c'est pas dans son interet de merger grsec dans linux, ça casse son business

Re: Chantage

Posté par Victor STINNER (page perso) le 06/01/09 à 20:43. Évalué à 10.

Si j'étais un sponsor, j'exigerai qu'il travaille main dans la main avec les développeurs noyau et qu'une partie soient accepté upstream avant un certain délai sinon je ne donne plus de sous. Hop, chantage, mais dans l'autre sens :-)

Bon

Posté par David Carlier le 06/01/09 à 22:18. Évalué à 10.

Espérons qu'ils vont pas tuer leur femme hein ...
Ok ====>[]