
Le logiciel libre en sécurité informatique.

Cédric Blancher <blancher@cartel-securite.fr>

—

9 juillet 2002

- Le besoin de sécurité

 - Pourquoi fait-on de la sécurité ?

 - Qu'est-ce qu'on attend d'un système de sécurité ?

- Le logiciel libre en sécurité

 - La problématique de confiance

 - Les atouts du logiciel libre

- Des faits concrets

- Le besoin de sécurité

Pourquoi fait-on de la sécurité ?

Qu'est-ce qu'on attend d'un système de sécurité ?

- Le logiciel libre en sécurité

La problématique de confiance

Les atouts du logiciel libre

- Des faits concrets

Pourquoi la sécurité ?

- ▶ Une problématique de confiance
 - Je me connecte à un monde inconnu
 - Je ne connais pas ce monde
 - Je ne fais pas confiance
- ➔ On ne fait confiance qu'à ce qu'on connaît

Un système de sécurité est le garant du fonctionnement du système d'information

- ▶ Bonne authentification
- ▶ Bonne gestion des accès
- ▶ Mise en application de procédés sûrs
- ▶ Interopérabilité forte
- ▶ Robustesse
- ▶ Suivi et pérennité du produit

- Le besoin de sécurité

Pourquoi fait-on de la sécurité ?

Qu'est-ce qu'on attend d'un système de sécurité ?

- Le logiciel libre en sécurité

La problématique de confiance

Les atouts du logiciel libre

- Des faits concrets

La problématique de confiance

- ▶ Le besoin de sécurité découle d'un manque de confiance
- ▶ Les outils de sécurité sont là pour imposer de la confiance
- ➔ On doit pouvoir faire confiance à notre implémentation

Jusqu'où peut-on faire confiance ?

- ▶ Le logiciel libre donne accès aux sources
- On peut vérifier la qualité du code source
- On peut adapter le code à ses besoins
- On gagne en indépendance et en liberté

Le problème du coût d'exploitation

- ▶ Le logiciel coûte moins cher
- ▶ Achat
- ▶ Exploitation et maintenance
- ▶ Mises à jour
- ➔ Un atout, mais globalement un faux problème

Où le logiciel propriétaire devrait prendre le dessus ?

- ▶ Qualité
- ▶ Garantie
- ▶ Suivi
- ▶ Pérennité
- ➔ Aucun de ces points n'est assuré

Le secret ne garantit pas la sécurité

- ▶ On trouve de toute manière les failles
- ▶ La découverte n'est pas forcément plus lente

L'ouverture est une forme de garantie

- ▶ Audit du code
 - ▶ Évolution
 - ▶ Pérennité
 - ▶ Suivi
- ➔ Le logiciel propriétaire permet ceci, mais à quel prix ?

Science sans conscience n'est que ruine de l'âme

- ▶ Le logiciel libre permet d'appréhender les concepts mis en jeu
- ▶ Le logiciel libre facilite l'ouverture vers des solutions plus perfectionnées
- ➔ Formidable outil d'appropriation des concepts et des outils

- Le besoin de sécurité

 - Pourquoi fait-on de la sécurité ?

 - Qu'est-ce qu'on attend d'un système de sécurité ?

- Le logiciel libre en sécurité

 - La problématique de confiance

 - Les atouts du logiciel libre

- Des faits concrets

Piratage de sites web (Attrition)

- ▶ Microsoft NT/2000 : 59%
- ▶ Linux : 21%
- ▶ Solaris : 8%
- ▶ *BSD : 6%

Nombre de failles (Bugtrack 1997-2000)

- ▶ Windows 9x/NT/2000 : 195 failles
- ▶ Solaris : 98 failles
- ▶ RedHat Linux : 96 failles
- ▶ Debian GNU/Linux : 54 failles
- ▶ OpenBSD : 14 failles

Durée de la période de vulnérabilité (Bugtrack 1999)

- ▶ RedHat : 11,23 jours (31 failles)
- ▶ Microsoft : 16,10 jours (61 failles)
- ▶ Solaris : 89,50 jours (8 failles)

Qualité des logiciels :

- ▶ Nessus a été élu meilleur scanner de vulnérabilité en 2001

Des faits concrets pour opposer logiciel libre et logiciel propriétaire

➔ http://www.dwheeler.com/oss_fs_why.html

Conclusion :

La sécurité impose :

- ▶ Transparence
 - ▶ Sûreté
 - ▶ Indépendance
- ➔ Le logiciel libre est la seule solution qui réponde à ces contraintes