

Sécuriser votre système GNU/Linux



Par **Achraf cherti** (*aka Asher256*)



<http://achraf.cherti.name/>

Plan Général

- Pourquoi faire attention à votre sécurité ?
- Sécuriser votre **BIOS**
- Sécuriser votre **systeme GNU/Linux**
- Quelques sites web pour **aller plus loin**
- Vos questions

Pourquoi faire attention à votre sécurité ?

- Protéger vos mots de passe : courriel, messagerie instantannée, administration de votre blog, etc.
- Protéger vos données personnelles : photos, vidéos, textes, etc.
- Protéger les données de vos projets : plan, maquettes, codes source non libres, etc.

Vous laisseriez n'importe qui accéder à vos données ?

Pourquoi faire attention à votre sécurité ?

Un débutant pourrait vous pirater !

Peut être appliqué à la majorité des ordinateurs de bureau non sécurisés

- Ceci est un exemple simple pour vous montrer les détails qu'on ignore parfois !
- Il suffirait à n'importe qui de booter avec un Live CD, accéder à votre disque dur et modifier votre mot de passe administrateur.
- Après un redémarrage, il aurait un accès complet à votre machine.

Pourquoi faire attention à votre sécurité ?

Pourquoi vous pirater ?

- Utiliser votre ordinateur pour en pirater d'autres : vous participerez peut-être à une activité dont vous ne serez pas fiers
- Avoir vos données confidentielles : numéro de carte bancaire, mots de passe, données sensibles (code source non libre)
- Profiter de votre bande passante : connexion Internet très lente pour vous

Plan Général

- Pourquoi faire attention votre sécurité ?
- **Sécuriser votre BIOS**
- Sécuriser votre **systeme GNU/Linux**
- Quelques sites web pour **aller plus loin**
- Vos questions

Sécuriser votre BIOS

- Mettre un mot de passe pour empêcher la modification des paramètres du BIOS
- Facultatif : mettre un mot de passe pour protéger le démarrage de la machine
- Ne pas laisser la possibilité de booter par autre chose que le disque contenant votre système GNU/Linux : désactiver le boot depuis les clés USB, CD-ROM...
- Protéger physiquement la machine : pour éviter que la pile CMOS soit retirée

Sécuriser votre ordinateur de bureau

Les mises à jour, c'est important

Faites attention aux mises à jour de votre système, nombreuses failles critiques sont corrigées. Vérifiez régulièrement ces dernières ou utilisez un programme qui vous notifie quand des mises à jour sont disponible.



Sécuriser votre ordinateur de bureau

Quand vous installez un programme...

- Pour les paquets, **utilisez les dépôts officiels** : pas de paquet à droite et à gauche, pas de compilation depuis les codes source, etc.
- Éviter tout ce qui n'est pas « paquet » : les scripts qui vous installent un programme, les installeurs automatiques (similaires à ceux de Windows), etc. Ils salissent le système car ils ne sont pas gérés par la communauté et peuvent faire n'importe quoi dans votre système de fichiers (par exemple donner les mauvais droits à un fichier exécutable).

Sécuriser votre ordinateur de bureau

Bloquez votre écran !

- Activez l'écran de veille et activez le fait que ce dernier soit protégé par un mot de passe
- CTRL+L est généralement utilisé pour bloquer votre écran (sous GNOME par exemple)
- Si votre bureau ne permet pas cela (par exemple Fluxbox), je vous recommande d'utiliser le programme **xlock**
- Si vous utilisez le terminal, il est aussi possible de « bloquer votre écran ». Utilisez **vlock** avec l'option **-a**. Par exemple : **vlock -a**

Sécuriser votre ordinateur de bureau

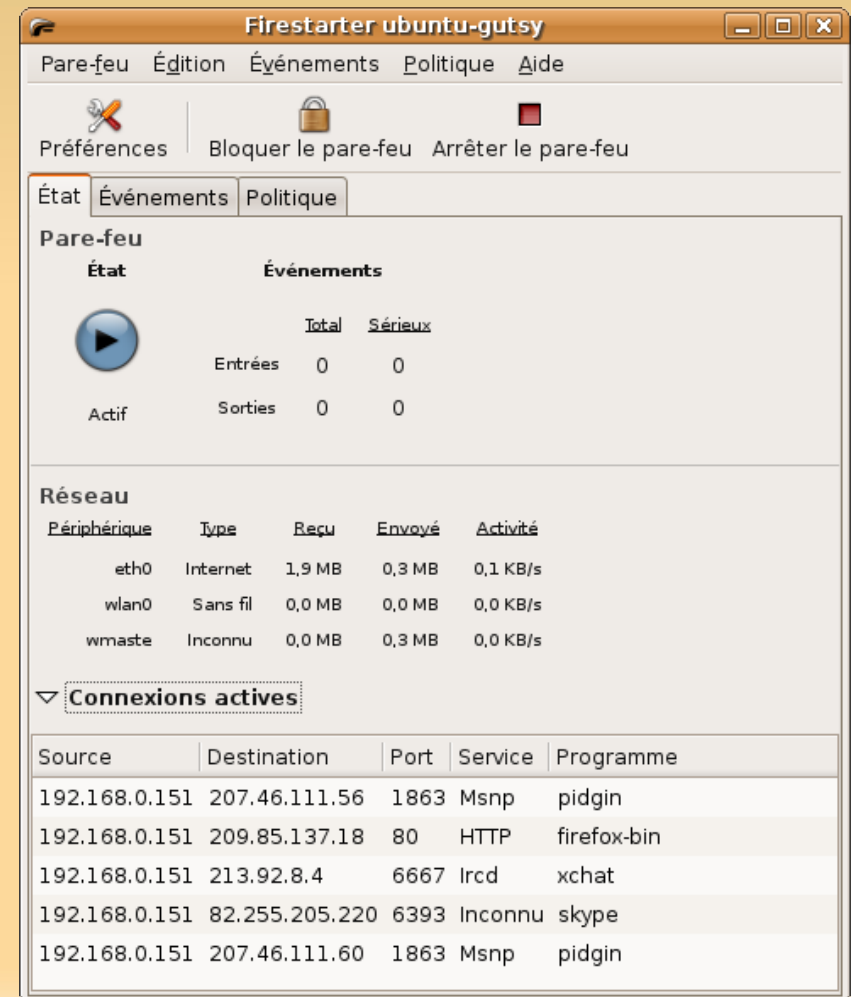
Utilisez un pare-feu !

- Un processus de votre système est peut-être en train d'écouter des requêtes dans des ports ? Pour vous en assurer, lancez la commande en tant que root :
lsof -i -n | grep -i LISTEN
- Quoi qu'il en soit, que votre ordinateur ait des programmes qui écoutent ou non, il est important de filtrer les données qui transitent !
- Sous GNU/Linux, un pare-feu est intégré au noyau (iptables), mais il est difficile à utiliser, c'est pour cette raison qu'il y a des « interfaces » comme Firestarter ou Shorewall (je recommande ce dernier pour une utilisation avancée) qui ont été faites

Sécuriser votre ordinateur de bureau

Utilisez un pare-feu : Firestarter

- Interface user-friendly
- Accessible aux débutants
- Permet le blocage des ports et le partage de la connexion Internet très facilement



Sécuriser votre ordinateur de bureau

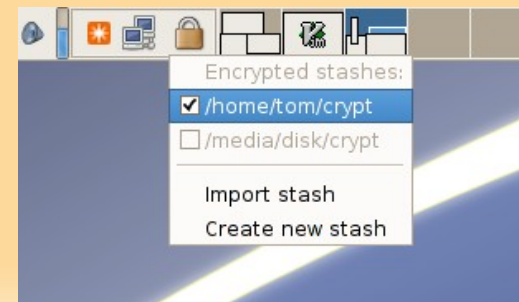
Chiffrer le contenu d'un répertoire

- Utiliser **encfs** qui permet de monter un répertoire source dans un répertoire destination dans l'espace utilisateur.

Exemple :

```
encfs /home/achraf/chiffre /home/achraf/dechiffre
```

- Pour utiliser simplement **encfs**, je vous recommande l'interface graphique **cryptkeeper** qui se loge dans la barre des status pour vous donner un accès rapide à vos répertoires chiffrés avec encfs.



Sécuriser votre ordinateur de bureau

Chiffrer tout le disque avec dm-crypt

- En cas de vol, le contenu du disque est illisible
- Pour lire le contenu du disque, il faut avoir la clé (parfois en forme de mot de passe)
- Je recommande pour les **utilisateurs avancés** sur le Wiki Gentoo : <http://tinyurl.com/5efert>
- **Pour les débutants**, installez une Debian ou une Ubuntu (alternate) pour avoir un disque dur chiffré **configuré automatiquement par l'installateur !**

Sécuriser votre ordinateur de bureau

Mot de passe dans GRUB

- GRUB c'est le menu que vous avez au démarrage pour choisir le système à démarrer : Windows, GNU/Linux, etc.
- Par défaut, la modification des paramètres passés au noyau est permise pour tout le monde, en tapant la touche 'e', chose qui pourrait être utilisée à l'avantage du pirate (booter en mode recovery par exemple).
- **La solution est de mettre un mot de passe** pour ne permettre la modification qu'après avoir entré ce dernier.

Sécuriser votre ordinateur de bureau

Mot de passe dans GRUB :
liens pour le faire

- Sous Debian ou Ubuntu, je recommande : <http://tinyurl.com/5arxka>
- Je recommande aussi cette documentation générale <http://tinyurl.com/6l7vy6>

Sécuriser votre ordinateur de bureau

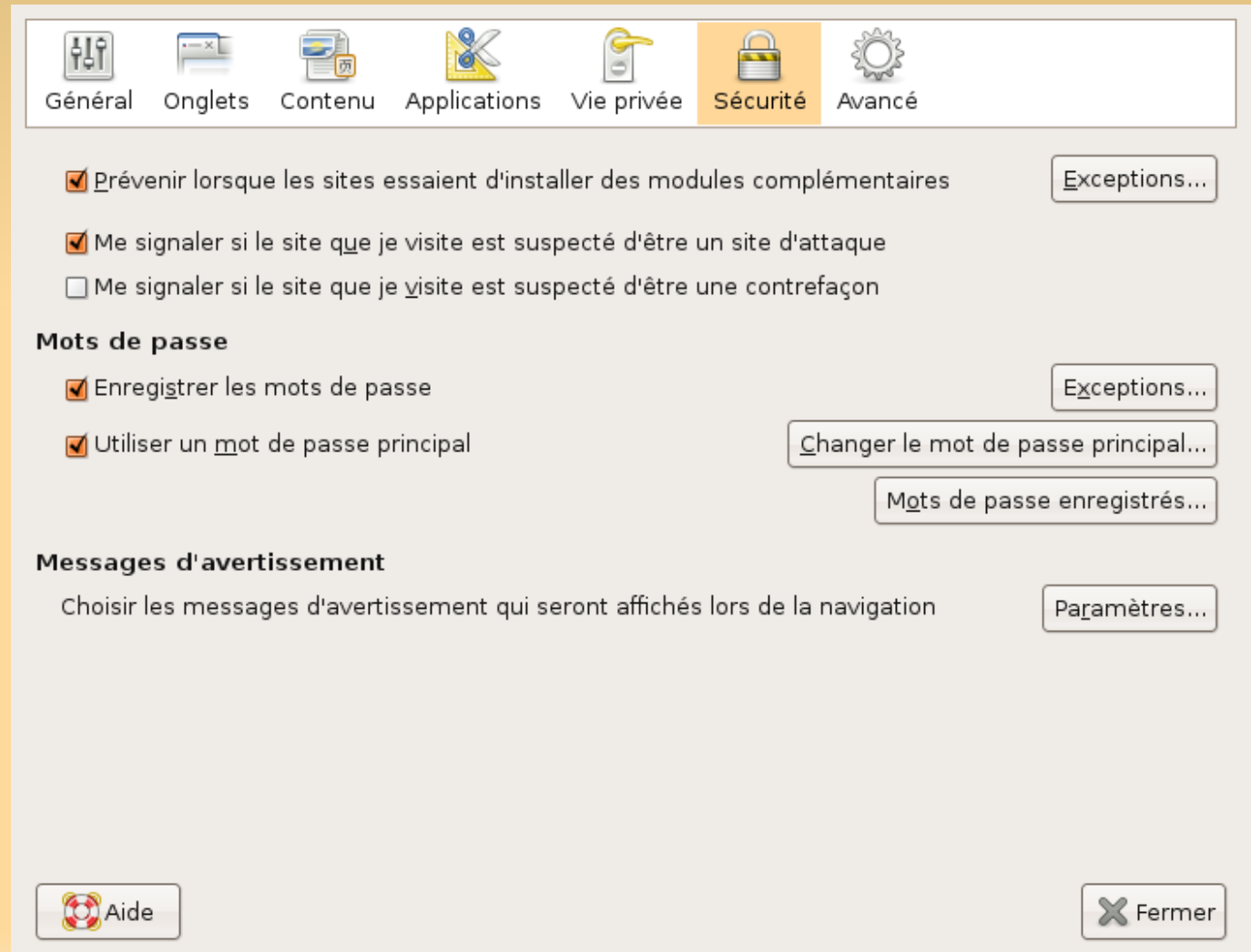
Navigation plus sûre avec Firefox

- Comment protéger vos mots de passe ?
- Comment protéger votre vie privée : historique, cache, cookies, etc.
- Je vais vous recommander quelques extensions, pour rendre votre navigateur Firefox beaucoup plus sécurisé.

Sécuriser votre ordinateur de bureau

Firefox : voir mots de passes

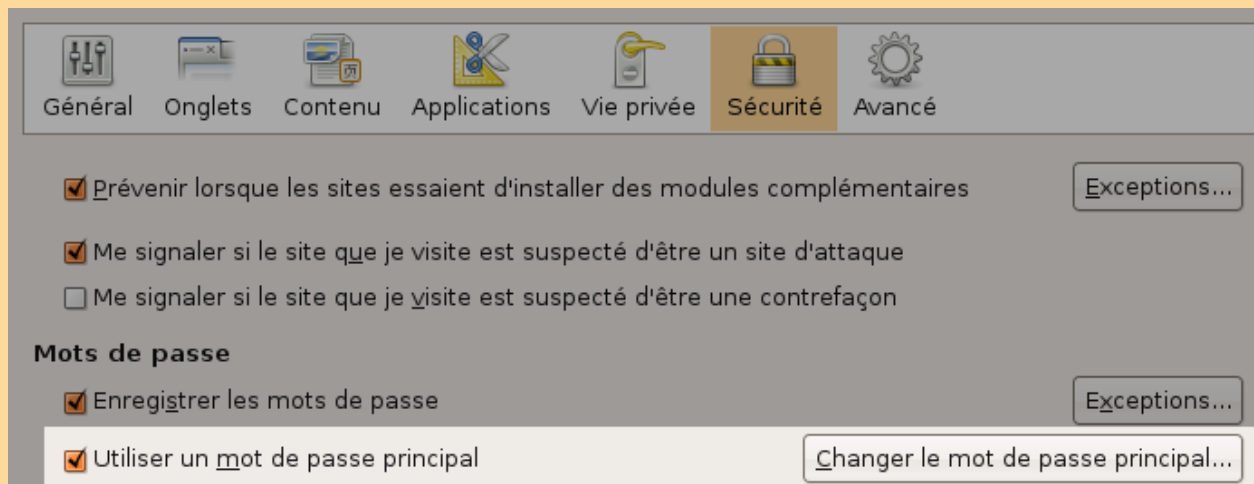
Pour voir vos mots de passes **en clair**, cliquez sur le menu **Édition** puis le sous-menu **Préférences**, choisissez l'onglet **Sécurité** (voir capture à droite) puis cliquez sur « **Mots de passe enregistrés** ».



Sécuriser votre ordinateur de bureau

Firefox: protéger vos mots de passe

- Cliquez sur le menu **Édition** puis choisissez **Préférences**. Dans la nouvelle fenêtre, cliquez sur l'onglet « **sécurité** »
- Cochez la case « **Utiliser un mot de passe principal** »
- Cliquez sur le bouton « **Changer le mot de passe principal** »



Un mot de passe principal sert à protéger des informations sensibles comme les mots de passe utilisés sur les sites. Si vous en créez un, il vous sera demandé de l'introduire une fois par session lorsque Firefox accède aux informations enregistrées protégées par ce mot de passe.

Mot de passe actuel :

Entrez le nouveau mot de passe :

Réentrez le nouveau mot de passe :

Mesure de la qualité du mot de passe



Faites attention à ne pas oublier le mot de passe principal. Si vous l'oubliez, vous n'aurez plus accès aux informations qu'il protège.

Sécuriser votre ordinateur de bureau

Firefox : vider les informations

- Cliquez sur le menu **Édition** puis choisissez le sous-menu **Préférences**. Dans la nouvelle fenêtre, cliquez sur l'onglet « **vie privée** »
- Cochez la case « **toujours effacer mes informations personnelles à la fermeture de Firefox** »
- Cliquez sur « **Paramètres** » pour personnaliser ce qui sera effacé (je recommande de laisser uniquement « **mots de passe enregistrés** », pour les moins paranos, vous pouvez laisser les cookies et la cache)

Vie privée

Toujours effacer mes informations personnelles à la fermeture de Firefox

Paramètres...

Demander avant d'effacer mes traces



Effacer mes traces maintenant...

Sécuriser votre ordinateur de bureau

Conseils en vrac

- Mettre dans votre `~/.bashrc` :
 `export TMOUT=60`
 `alias rm="rm -i"`
- Préférer les programmes utilisant un portefeuille de mots de passe (GNOME keyring ou Kwallet)
- Installer TOR, pour cacher son adresse IP
<http://www.torproject.org/index.html.fr>
- Soyez le seul à utiliser votre session utilisateur

Sécuriser votre ordinateur de bureau

Conseils rapides pour vos serveurs

- Ne jamais lancer un serveur en tant que root
- Vérifier l'intégrité de votre disque avec un outil comme **integrit**
- Garder l'oeil sur votre système avec les programmes : **tiger**, **logwatch** et **logcheck**
- Installer des détecteurs d'intrusion comme **snort**
- Changer les ports par défaut des serveurs, de préférence plus de 10000. Par exemple 22500 pour SSH.
- Installer des anti-rootkit : **rkhunter** et **chkrootkit**

Plan Général

- Pourquoi faire attention votre sécurité ?
- Sécuriser votre **BIOS**
- Sécuriser votre **systeme GNU/Linux**
- Quelques sites web pour **aller plus loin**
- Vos questions

Quelques sites web pour aller plus loin

- Securing Debian Howto
<http://tinyurl.com/yf7hmz>
- Security Howto
<http://tinyurl.com/5j753y>
- Gentoo Security Handbook
<http://tinyurl.com/696pvr>
- Security Quick Start Howto
<http://tinyurl.com/6bsaju>

Plan Général

- Pourquoi faire attention votre sécurité ?
- Sécuriser votre **BIOS**
- Sécuriser votre **ordinateur de bureau**
- Sécuriser votre **serveur**
- Quelques sites web pour **aller plus loin**
- **Vos questions**

Merci de votre attention !

Avez-vous des questions ?



Contact :

<http://achraf.cherti.name/contact.html>