Cryptologie et sécurité en pratique

Christophe Guyeux

IUT de Belfort-Montbéliard, Université de Franche-Comté

Cours de Mathématiques et Informatique, 2008

Avant-propos

- On présente quelques outils fournissant des fonctions cryptographiques ou de sécurité.
- On en profite pour parler de certificats.

Sources

Les informations de ce cours ont principalement été récupérées sur les sites suivants :

- Comment ça marche.
- Ubuntu-fr.org.
- Wikipedia.
- Linuxfr.org

Plan

Les certificats

Introduction à la notion de certificat

Raison d'être des certificats

- Les algorithmes de chiffrement asymétrique sont basés sur le partage entre les différents utilisateurs d'une clé publique.

Raison d'être des certificats

- Les algorithmes de chiffrement asymétrique sont basés sur le partage entre les différents utilisateurs d'une clé publique.
- Généralement le partage de cette clé se fait au travers d'un annuaire électronique (généralement au format LDAP) ou bien d'un site web.

Raison d'être des certificats

- Les algorithmes de chiffrement asymétrique sont basés sur le partage entre les différents utilisateurs d'une clé publique.
- Généralement le partage de cette clé se fait au travers d'un annuaire électronique (généralement au format LDAP) ou bien d'un site web.
- Toutefois ce mode de partage a une grande lacune : rien ne garantit que la clé est bien celle de l'utilisateur à qui elle est associée.

Où apparaît le certificat

- En effet un pirate peut corrompre la clé publique présente dans l'annuaire en la remplaçant par sa clé publique.

Où apparaît le certificat

- En effet un pirate peut corrompre la clé publique présente dans l'annuaire en la remplaçant par sa clé publique.
- Ainsi, le pirate sera en mesure de déchiffrer tous les messages ayant été chiffrés avec la clé présente dans l'annuaire.

Où apparaît le certificat

- En effet un pirate peut corrompre la clé publique présente dans l'annuaire en la remplaçant par sa clé publique.
- Ainsi, le pirate sera en mesure de déchiffrer tous les messages ayant été chiffrés avec la clé présente dans l'annuaire.
- Le certificat permet d'associer une clé publique à une entité (une personne, une machine, ...) afin d'en assurer la validité.

Autorité de certification

- Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé autorité de certification (souvent notée CA pour Certification Authority).

Autorité de certification

- Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé autorité de certification (souvent notée CA pour Certification Authority).
- L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité (équivalent à la date limite de péremption des produits alimentaires).

Autorité de certification

- Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé autorité de certification (souvent notée CA pour Certification Authority).
- L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité (équivalent à la date limite de péremption des produits alimentaires).
- Elle peut aussi révoquer éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire).

Structure d'un certificat

- Les certificats sont des petits fichiers divisés en deux parties :
  - La partie contenant les informations
  - La partie contenant la signature de l'autorité de certification

Structure d'un certificat

- Les certificats sont des petits fichiers divisés en deux parties :
  - La partie contenant les informations
  - La partie contenant la signature de l'autorité de certification
- La structure des certificats est normalisée par le standard X.509 de l'UIT, qui définit les informations contenues dans le certificat...

Le standard X.509

1. La version de X.509 à laquelle le certificat correspond ;
2. Le numéro de série du certificat ;
3. L'algorithme de chiffrement utilisé pour signer le certificat ;
4. Le nom (DN, pour Distinguished Name) de l'autorité de certification émettrice ;
5. La date de début de validité du certificat ;
6. La date de fin de validité du certificat ;
7. L'objet de l'utilisation de la clé publique ;
8. La clé publique du propriétaire du certificat ;
9. La signature de l'émetteur du certificat (thumbprint).

La signature du CA

- L'ensemble de ces informations (informations + clé publique du demandeur) est signé par l'autorité de certification.

La signature du CA

- L'ensemble de ces informations (informations + clé publique du demandeur) est signé par l'autorité de certification.
- Cela signifie qu'une fonction de hachage crée une empreinte de ces informations.

La signature du CA

- L'ensemble de ces informations (informations + clé publique du demandeur) est signé par l'autorité de certification.
- Cela signifie qu'une fonction de hachage crée une empreinte de ces informations.
- Ce condensé est chiffré à l'aide de la clé privée de l'autorité de certification.

La signature du CA

- L'ensemble de ces informations (informations + clé publique du demandeur) est signé par l'autorité de certification.
- Cela signifie qu'une fonction de hachage crée une empreinte de ces informations.
- Ce condensé est chiffré à l'aide de la clé privée de l'autorité de certification.
- La clé publique ayant été préalablement largement diffusée afin de permettre aux utilisateurs de vérifier la signature avec la clé publique de l'autorité de certification.

Utilisation du certificat

- Lorsqu'un utilisateur désire communiquer avec une autre personne, il lui suffit de se procurer le certificat du destinataire.

Utilisation du certificat

- Lorsqu'un utilisateur désire communiquer avec une autre personne, il lui suffit de se procurer le certificat du destinataire.
- Ce certificat contient le nom du destinataire, ainsi que sa clé publique et est signé par l'autorité de certification.

Utilisation du certificat

- Lorsqu'un utilisateur désire communiquer avec une autre personne, il lui suffit de se procurer le certificat du destinataire.
- Ce certificat contient le nom du destinataire, ainsi que sa clé publique et est signé par l'autorité de certification.
- Il est donc possible de vérifier la validité du message :
  - en appliquant d'une part la fonction de hachage aux informations contenues dans le certificat,
  - en déchiffrant d'autre part la signature de l'autorité de certification avec la clé publique de cette dernière,
  - et en comparant ces deux résultats.

Les certificats

Introduction à SSL

Présentation de SSL

- SSL (Secure Sockets Layers - Couche de sockets sécurisée) est un procédé de sécurisation des transactions effectuées via Internet.

Présentation de SSL

- SSL (Secure Sockets Layers - Couche de sockets sécurisée) est un procédé de sécurisation des transactions effectuées via Internet.
- Le standard SSL a été mis au point par Netscape, en collaboration avec Mastercard, Bank of America, MCI et Silicon Graphics.

Présentation de SSL

- SSL (Secure Sockets Layers - Couche de sockets sécurisée) est un procédé de sécurisation des transactions effectuées via Internet.
- Le standard SSL a été mis au point par Netscape, en collaboration avec Mastercard, Bank of America, MCI et Silicon Graphics.
- Il repose sur un procédé de cryptographie par clef publique afin de garantir la sécurité de la transmission de données sur internet.

Présentation de SSL

- SSL (Secure Sockets Layers - Couche de sockets sécurisée) est un procédé de sécurisation des transactions effectuées via Internet.
- Le standard SSL a été mis au point par Netscape, en collaboration avec Mastercard, Bank of America, MCI et Silicon Graphics.
- Il repose sur un procédé de cryptographie par clef publique afin de garantir la sécurité de la transmission de données sur internet.
- Son principe consiste à établir un canal de communication sécurisé (chiffré) entre deux machines (un client et un serveur) après une étape d'authentification.

SSL et protocoles

- Le système SSL est indépendant du protocole utilisé.

SSL et protocoles

- Le système SSL est indépendant du protocole utilisé.
- Cela signifie qu'il peut aussi bien sécuriser des transactions faites sur le Web par le protocole HTTP que des connexions via le protocole FTP, POP ou IMAP.

SSL et protocoles

- Le système SSL est indépendant du protocole utilisé.
- Cela signifie qu'il peut aussi bien sécuriser des transactions faites sur le Web par le protocole HTTP que des connexions via le protocole FTP, POP ou IMAP.
- En effet, SSL agit telle une couche supplémentaire, permettant d'assurer la sécurité des données, située entre la couche application et la couche transport (protocole TCP par exemple).

SSL et protocoles

- Le système SSL est indépendant du protocole utilisé.
- Cela signifie qu'il peut aussi bien sécuriser des transactions faites sur le Web par le protocole HTTP que des connexions via le protocole FTP, POP ou IMAP.
- En effet, SSL agit telle une couche supplémentaire, permettant d'assurer la sécurité des données, située entre la couche application et la couche transport (protocole TCP par exemple).
- De cette manière, SSL est transparent pour l'utilisateur.

Evolution du SSL

- La quasi intégralité des navigateurs supporte désormais le protocole SSL.

Evolution du SSL

- La quasi intégralité des navigateurs supporte désormais le protocole SSL.
- Au milieu de l'année 2001, le brevet de SSL appartenant jusqu'alors à Netscape a été racheté par l'IETF (Internet Engineering Task Force).

Evolution du SSL

- La quasi intégralité des navigateurs supporte désormais le protocole SSL.
- Au milieu de l'année 2001, le brevet de SSL appartenant jusqu'alors à Netscape a été racheté par l'IETF (Internet Engineering Task Force).
- Il a été rebaptisé pour l'occasion TLS (Transport Layer Security).

Les certificats

Fonctionnement de SSL 2.0

Introduction

- La sécurisation des transactions par SSL 2.0 est basée sur un échange de clés entre client et serveur.

Introduction

- La sécurisation des transactions par SSL 2.0 est basée sur un échange de clés entre client et serveur.
- La transaction sécurisée par SSL se fait selon le modèle suivant...

Le modèle

- Dans un premier temps, le client se connecte au site marchand sécurisé par SSL et lui demande de s'authentifier.

Le modèle

- Dans un premier temps, le client se connecte au site marchand sécurisé par SSL et lui demande de s'authentifier.
- Le client envoie également la liste des cryptosystèmes qu'il supporte, triée par ordre décroissant selon la longueur des clés.

Le modèle

- Dans un premier temps, le client se connecte au site marchand sécurisé par SSL et lui demande de s'authentifier.
- Le client envoie également la liste des cryptosystèmes qu'il supporte, triée par ordre décroissant selon la longueur des clés.
- Le serveur, à réception de la requête, envoie un certificat au client, contenant sa clé publique (au serveur) signée par une autorité de certification (CA).

Le modèle

- Dans un premier temps, le client se connecte au site marchand sécurisé par SSL et lui demande de s'authentifier.
- Le client envoie également la liste des cryptosystèmes qu'il supporte, triée par ordre décroissant selon la longueur des clés.
- Le serveur, à réception de la requête, envoie un certificat au client, contenant sa clé publique (au serveur) signée par une autorité de certification (CA).
- Il envoie aussi le nom du cryptosystème le plus haut dans la liste avec lequel il est compatible.

Le modèle

- La longueur de la clé de chiffrement sera celle du cryptosystème commun ayant la plus grande taille de clé.

Le modèle

- La longueur de la clé de chiffrement sera celle du cryptosystème commun ayant la plus grande taille de clé.
- Le client vérifie la validité du certificat (donc l'authenticité du marchand).

Le modèle

- La longueur de la clé de chiffrement sera celle du cryptosystème commun ayant la plus grande taille de clé.
- Le client vérifie la validité du certificat (donc l'authenticité du marchand).
- Puis il crée une clé secrète aléatoire (plus exactement un bloc prétenduement aléatoire)

Le modèle

- La longueur de la clé de chiffrement sera celle du cryptosystème commun ayant la plus grande taille de clé.
- Le client vérifie la validité du certificat (donc l'authenticité du marchand).
- Puis il crée une clé secrète aléatoire (plus exactement un bloc prétenduement aléatoire)
- Il chiffre cette clé à l'aide de la clé publique du serveur, puis lui envoie le résultat (la clé de session).

Le modèle

- Le serveur est en mesure de déchiffrer la clé de session avec sa clé privée.

Le modèle

- Le serveur est en mesure de déchiffrer la clé de session avec sa clé privée.
- Ainsi, les deux entités sont en possession d'une clé commune dont ils sont seuls connaisseurs.

Le modèle

- Le serveur est en mesure de déchiffrer la clé de session avec sa clé privée.
- Ainsi, les deux entités sont en possession d'une clé commune dont ils sont seuls connaisseurs.
- Le reste des transactions peut se faire à l'aide de clé de session, garantissant l'intégrité et la confidentialité des données échangées.

Des outils de cryptage

GtkHash

Présentation de GthHash

- Il existe des applications graphiques permettant de hacher du texte (ou des fichiers).

Présentation de GthHash

- Il existe des applications graphiques permettant de hacher du texte (ou des fichiers).
- On présente ici une application libre pour Ubuntu : GtkHash.

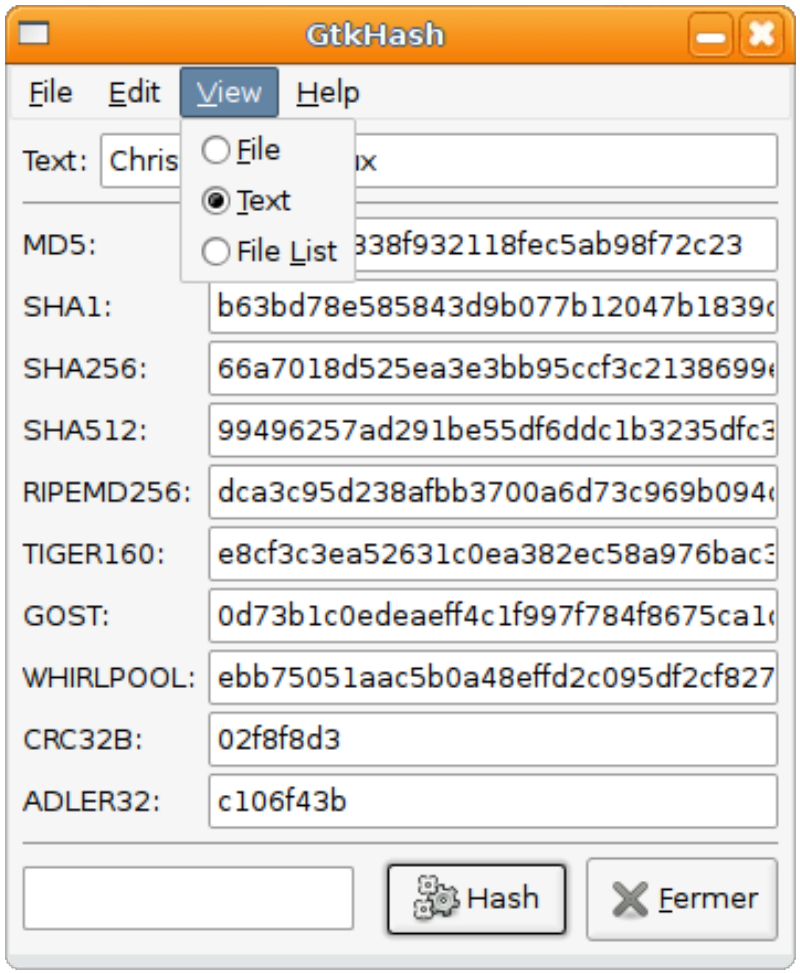
Présentation de GthHash

- Il existe des applications graphiques permettant de hacher du texte (ou des fichiers).
- On présente ici une application libre pour Ubuntu : GtkHash.
- Elle permet d'appliquer un bon nombre d'algorithmes de hachage, sur du texte ou des fichiers.

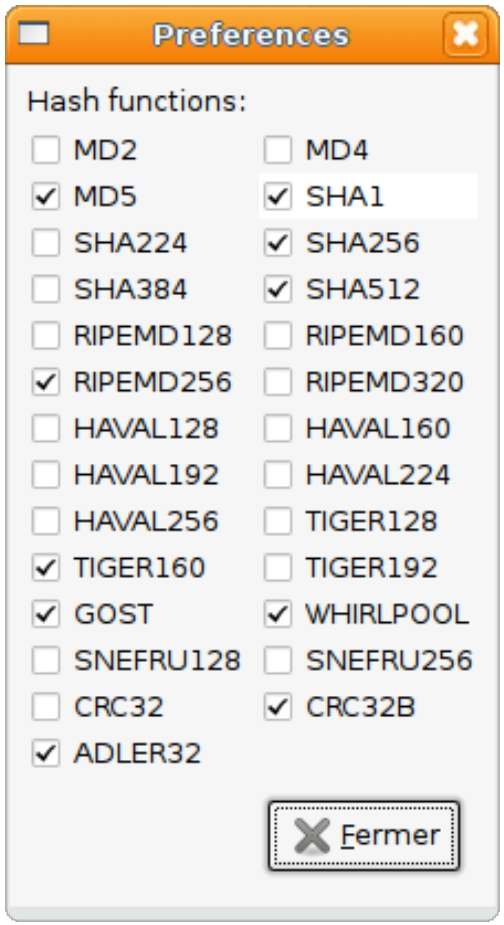
Présentation de GthHash

- Il existe des applications graphiques permettant de hacher du texte (ou des fichiers).
- On présente ici une application libre pour Ubuntu : GtkHash.
- Elle permet d'appliquer un bon nombre d'algorithmes de hachage, sur du texte ou des fichiers.
- On peut la récupérer ici : http ://www.gtkfiles.org/app.php/GtkHash

Gtkhash : les possibilités



Gtkhash : les algorithmes



Des outils

Cryptkeeper

Présentation de Cryptkeeper

- Cryptkeeper permet de créer des répertoires cryptés.

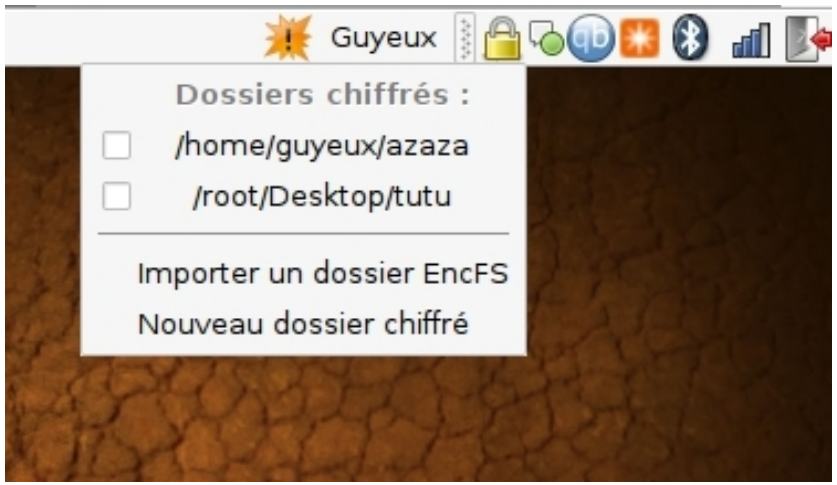
Présentation de Cryptkeeper

- Cryptkeeper permet de créer des répertoires cryptés.
- Vous avez alors une icone dans la barre des tâches, dans laquelle vous pouvez cocher les répertoires à monter.

Présentation de Cryptkeeper

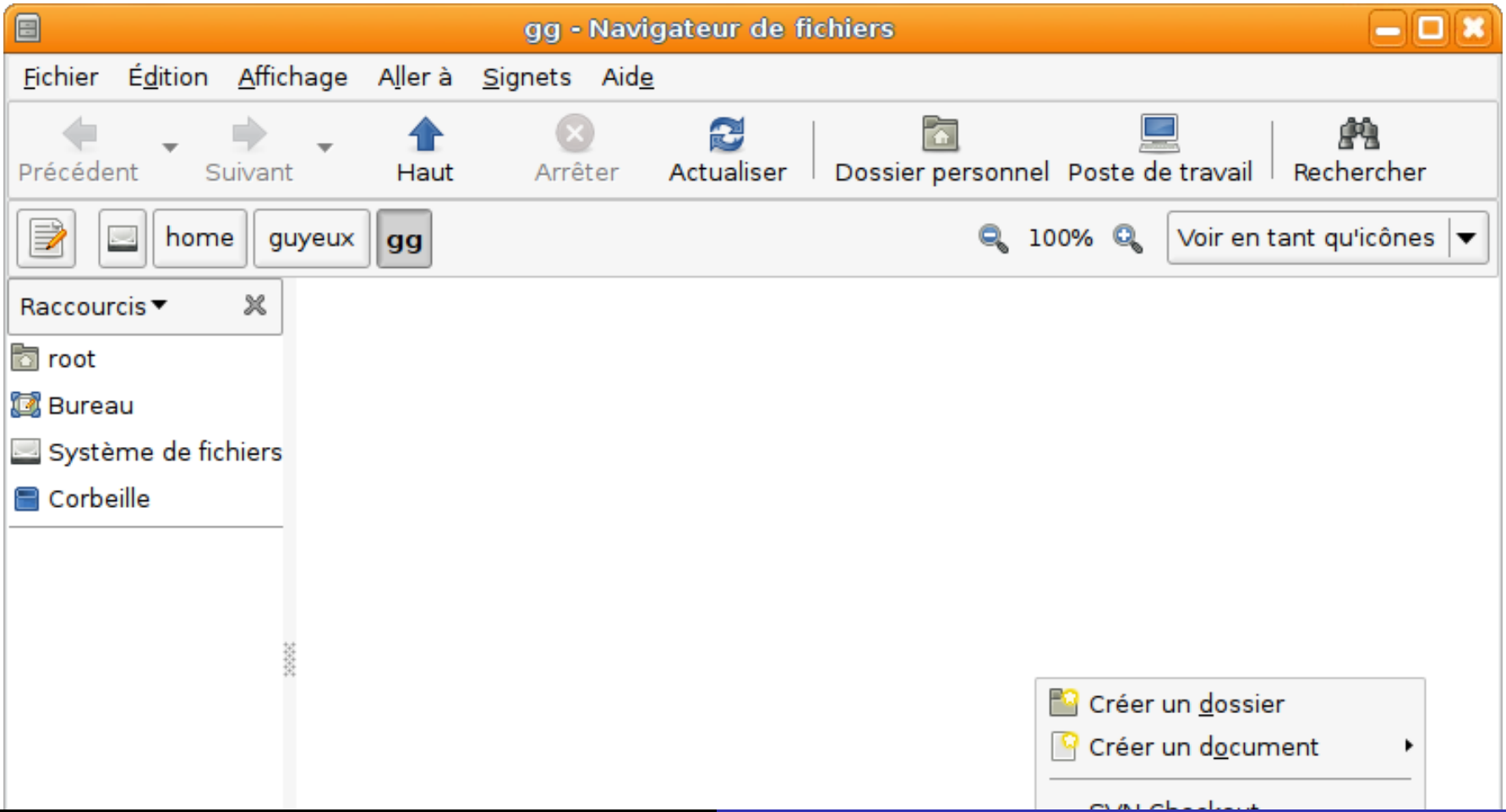
- Cryptkeeper permet de créer des répertoires cryptés.
- Vous avez alors une icone dans la barre des tâches, dans laquelle vous pouvez cocher les répertoires à monter.
- Un mot de passe vous sera alors demandé, puis le répertoire s'ouvrira dans Nautilus.

Cryptkeeper



Cryptkeeper

Cryptkeeper



Des outils

Seahorse

Présentation de Seahorse

- Seahorse est un logiciel assez complet de signature et chiffrement.

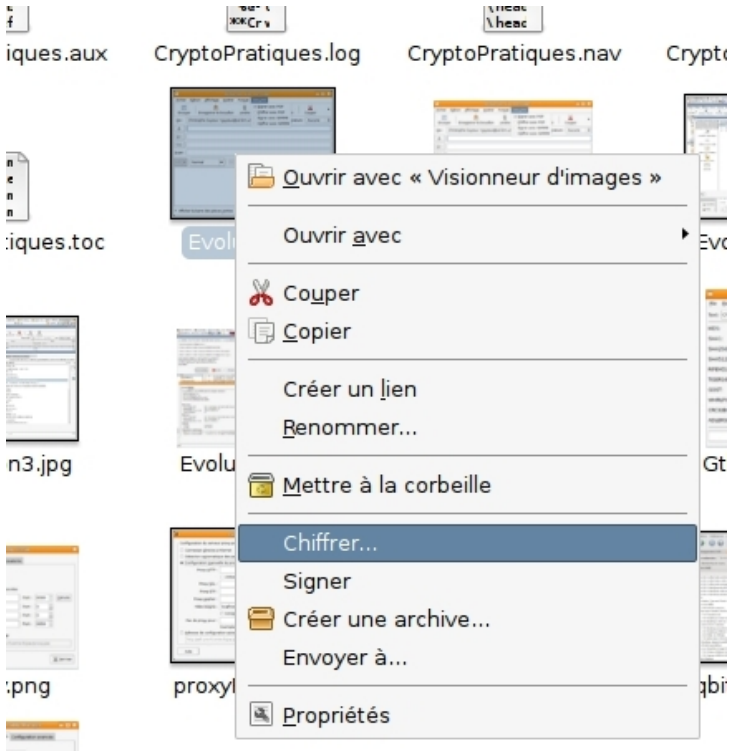
Présentation de Seahorse

- Seahorse est un logiciel assez complet de signature et chiffrement.
- Il vous permet de générer une clé publique/privée, de la déposer sur un serveur, ou d'importer une clé d'un ami.

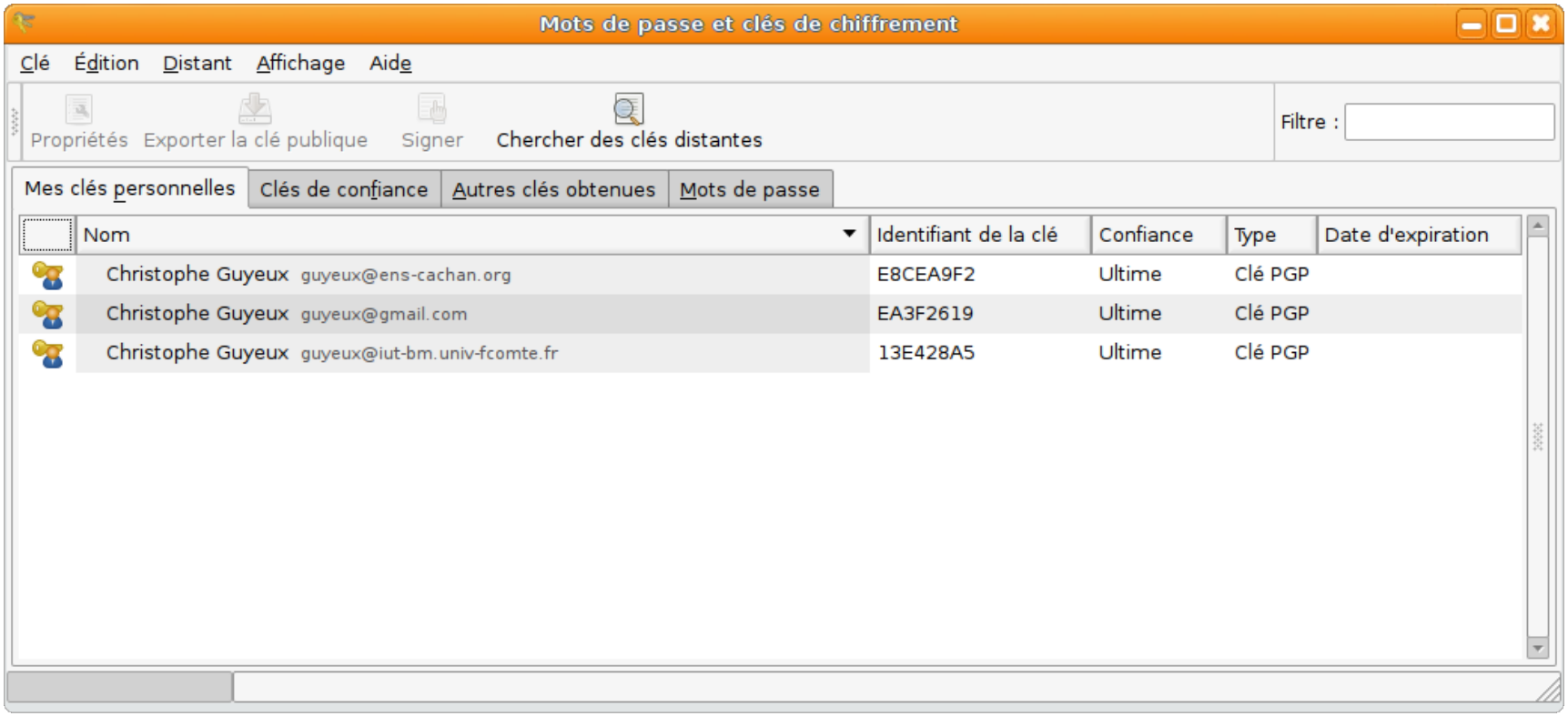
Présentation de Seahorse

- Seahorse est un logiciel assez complet de signature et chiffrement.
- Il vous permet de générer une clé publique/privée, de la déposer sur un serveur, ou d'importer une clé d'un ami.
- Il permet encore de chiffrer ou signer un fichier, voire le contenu du presse-papier.

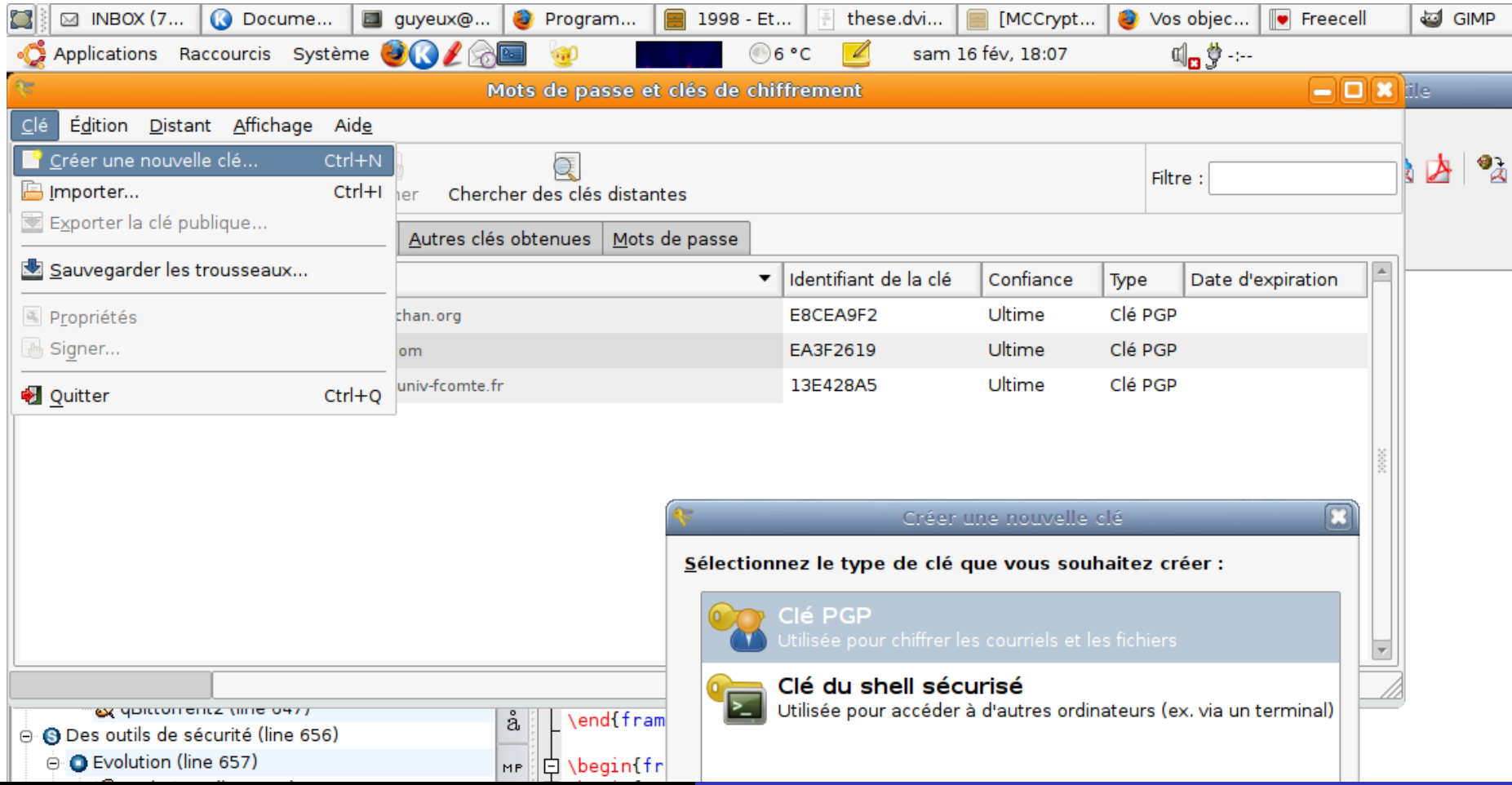
Seahorse


iques.aux
CryptoPratiques.log
CryptoPratiques.nav
iques.toc
n3.jpg
Evolu
:png
proxyl
Ouvrir avec « Visionneur d'images »
Ouvrir avec
Couper
Copier
Créer un lien
Renommer...
Mettre à la corbeille
Chiffrer...
Signer
Créer une archive...
Envoyer à...
Propriétés

Seahorse


Mots de passe et clés de chiffrement
Clé Édition Distant Affichage Aide
Propriétés
Exporter la clé publique
Signer
Chercher des clés distantes
Filtre :
Mes clés personnelles
Clés de confiance
Autres clés obtenues
Mots de passe
Nom
Identifiant de la clé
Confiance
Type
Date d'expiration
Christophe Guyeux guyeux@ens-cachan.org E8CEA9F2 Ultime Clé PGP
Christophe Guyeux guyeux@gmail.com EA3F2619 Ultime Clé PGP
Christophe Guyeux guyeux@iut-bm.univ-fcomte.fr 13E428A5 Ultime Clé PGP

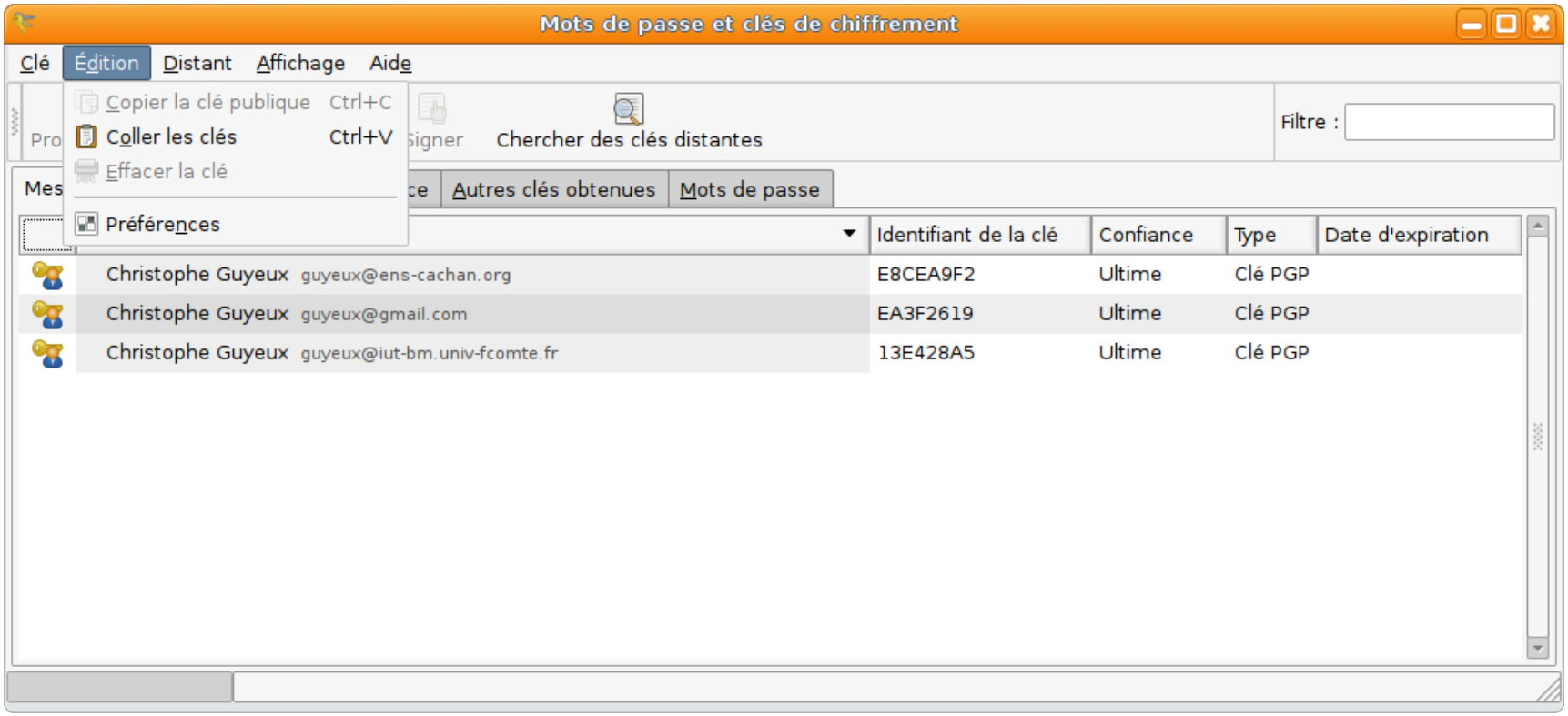
Seahorse


Mots de passe et clés de chiffrement
Clé
Édition
Distant
Affichage
Aide
Créer une nouvelle clé... Ctrl+N
Importer... Ctrl+I
Exporter la clé publique...
Sauvegarder les trousseaux...
Propriétés
Signer...
Quitter Ctrl+Q
Chercher des clés distantes
Filtre :
Autres clés obtenues
Mots de passe
Identifiant de la clé
Confiance
Type
Date d'expiration
E8CEA9F2 Ultime Clé PGP
EA3F2619 Ultime Clé PGP
13E428A5 Ultime Clé PGP
Créer une nouvelle clé
Sélectionnez le type de clé que vous souhaitez créer :
Clé PGP
Utilisée pour chiffrer les courriels et les fichiers
Clé du shell sécurisé
Utilisée pour accéder à d'autres ordinateurs (ex. via un terminal)
Des outils de sécurité (line 656)
Evolution (line 657)

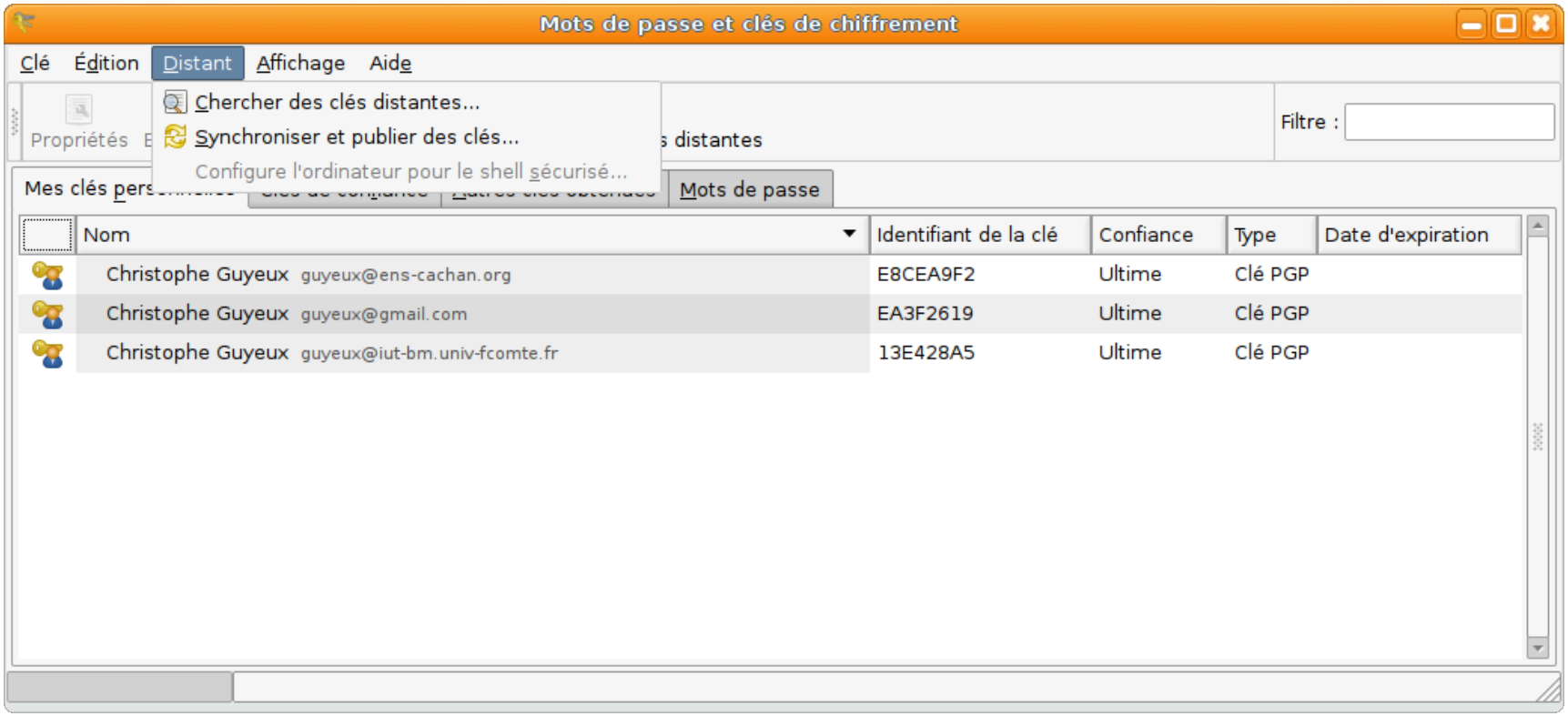
Seahorse


Nouvelle clé PGP
Une clé PGP vous permet de chiffrer des courriels ou des fichiers à destination d'autres personnes.
Nom complet :
Adresse électronique :
Commentaire :
Options avancées de clé
Type de chiffrement
DSA et ElGamal
Force de la clé (bits) :
2048
Date d'expiration :
15.02.2009
N'expire jamais
Aide
Annuler
Créer

Seahorse


Mots de passe et clés de chiffrement
Clé
Édition
Distant
Affichage
Aide
Copier la clé publique Ctrl+C
Coller les clés Ctrl+V
Effacer la clé
Préférences
Chercher des clés distantes
Filtre :
Autres clés obtenues
Mots de passe
Identifiant de la clé
Confiance
Type
Date d'expiration
Christophe Guyeux guyeux@ens-cachan.org E8CEA9F2 Ultime Clé PGP
Christophe Guyeux guyeux@gmail.com EA3F2619 Ultime Clé PGP
Christophe Guyeux guyeux@iut-bm.univ-fcomte.fr 13E428A5 Ultime Clé PGP

Seahorse


Mots de passe et clés de chiffrement
Clé
Édition
Distant
Affichage
Aide
Chercher des clés distantes...
Synchroniser et publier des clés...
Configure l'ordinateur pour le shell sécurisé...
Propriétés
Filtre :
Mots de passe
Nom
Identifiant de la clé
Confiance
Type
Date d'expiration
Christophe Guyeux guyeux@ens-cachan.org E8CEA9F2 Ultime Clé PGP
Christophe Guyeux guyeux@gmail.com EA3F2619 Ultime Clé PGP
Christophe Guyeux guyeux@iut-bm.univ-fcomte.fr 13E428A5 Ultime Clé PGP

Des outils

Des outils

Qbittorrent

Autres exemples

- Les outils informatiques que vous pouvez utiliser quotidiennement possedent parfois des fonctionnalités de cryptographie.

Autres exemples

- Les outils informatiques que vous pouvez utiliser quotidiennement possedent parfois des fonctionnalités de cryptographie.
- Par exemple, il existe une extension de chiffrement pour Pidgin (messagerie instantannée).

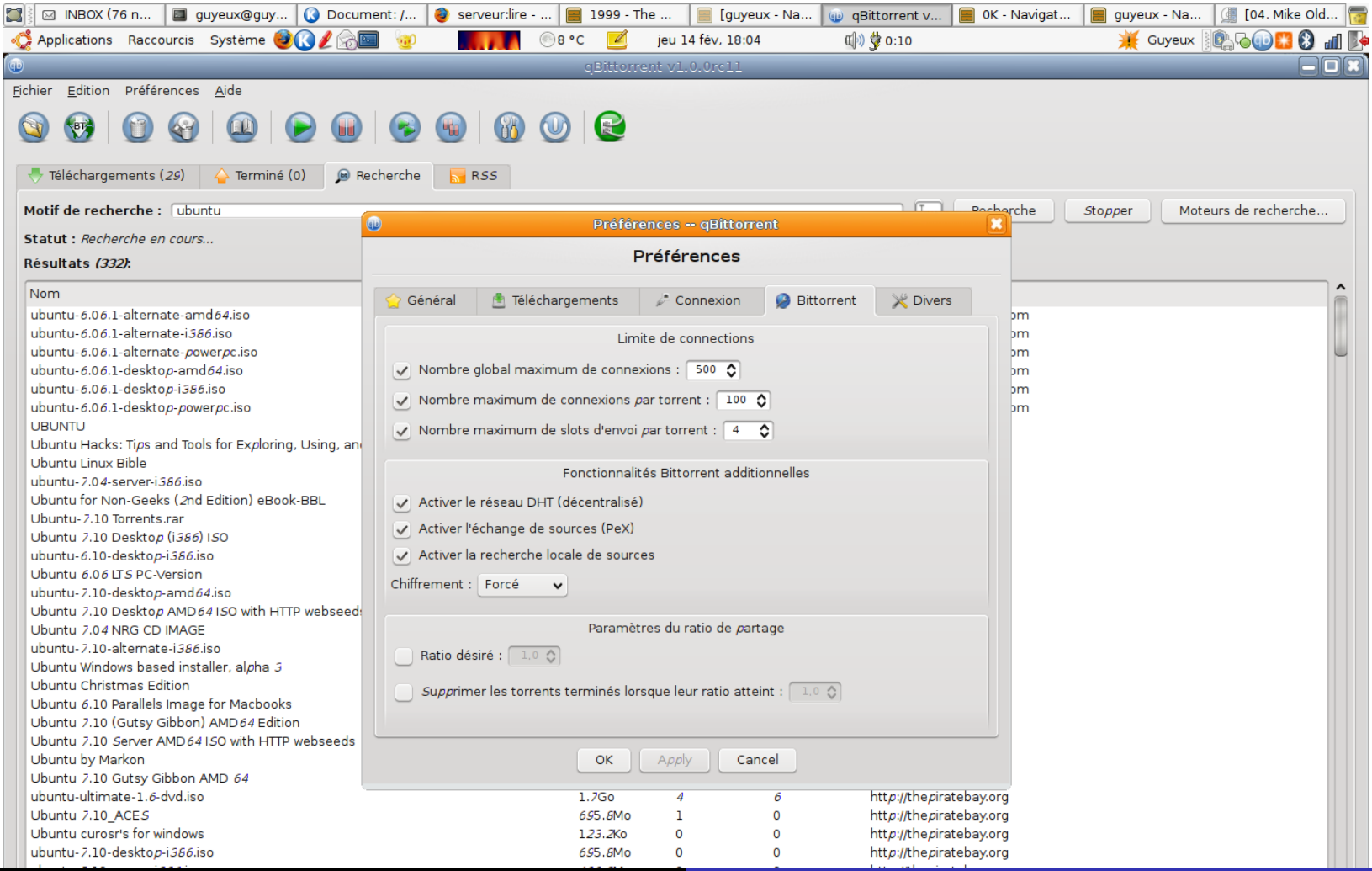
Autres exemples

- Les outils informatiques que vous pouvez utiliser quotidiennement possedent parfois des fonctionnalités de cryptographie.
- Par exemple, il existe une extension de chiffrement pour Pidgin (messagerie instantannée).
- On trouve aussi des éditeurs de texte qui permettent le chiffrement, ou la signature. Ainsi, une fois *seahorse* installé, vous pouvez faire ces actions avec gedit.

Autres exemples

- Les outils informatiques que vous pouvez utiliser quotidiennement possedent parfois des fonctionnalités de cryptographie.
- Par exemple, il existe une extension de chiffrement pour Pidgin (messagerie instantannée).
- On trouve aussi des éditeurs de texte qui permettent le chiffrement, ou la signature. Ainsi, une fois *seahorse* installé, vous pouvez faire ces actions avec gedit.
- D'autres sortes d'applications autorisent encore le chiffrement, comme le logiciel P2P *qbittorrent*...

Qbittorrent



Des outils de sécurité

Des outils de sécurité

Evolution

Présentation d'évolution

- On présente dans ce qui suit, à l'aide de captures d'écrans, différentes possibilités de la messagerie Evolutions, installée par défaut sous Ubuntu.

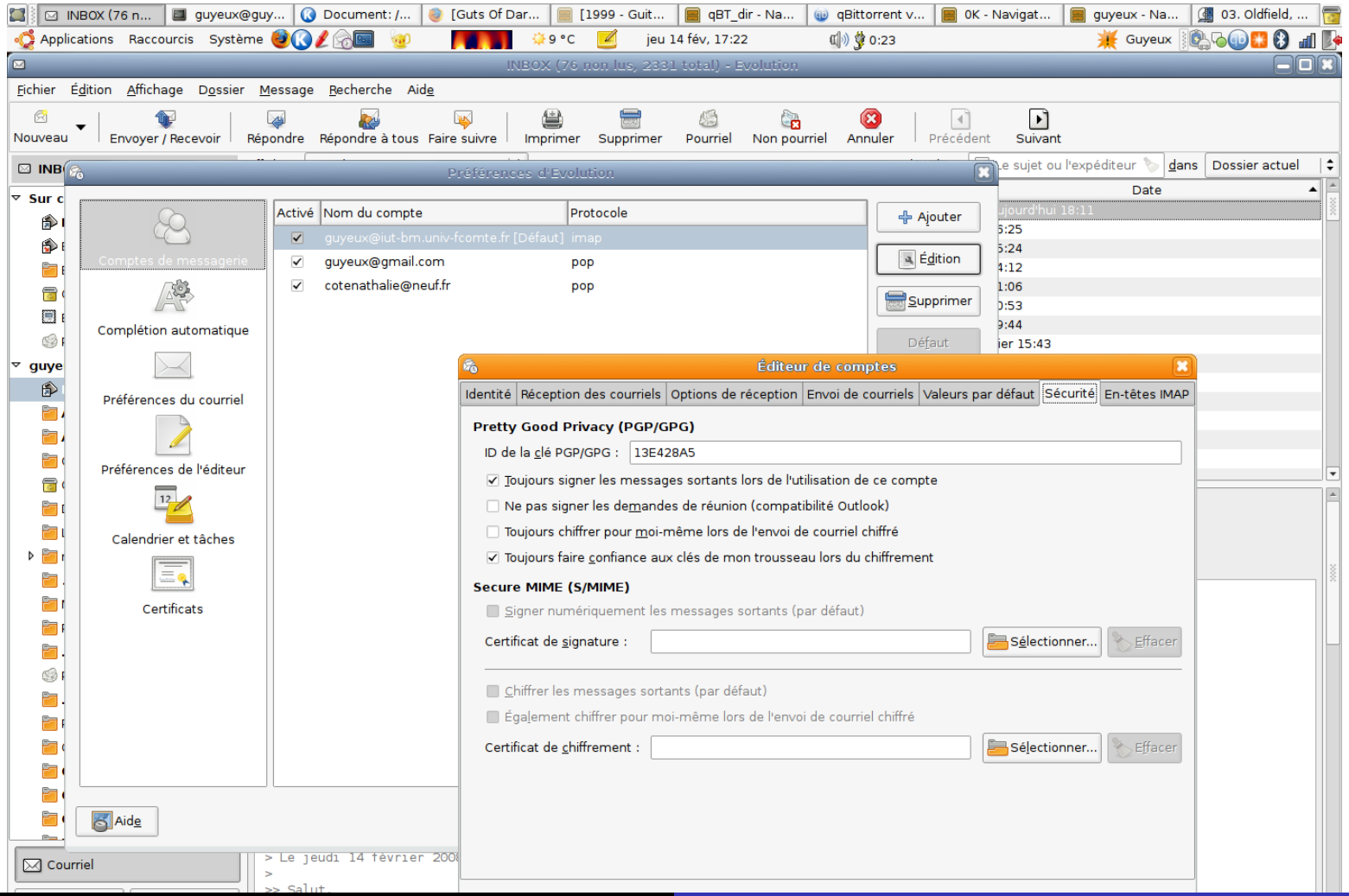
Présentation d'évolution

- On présente dans ce qui suit, à l'aide de captures d'écrans, différentes possibilités de la messagerie Evolutions, installée par défaut sous Ubuntu.
- On verra comment intégrer sa clé de chiffrement, et comment chiffrer ou signer un mail.

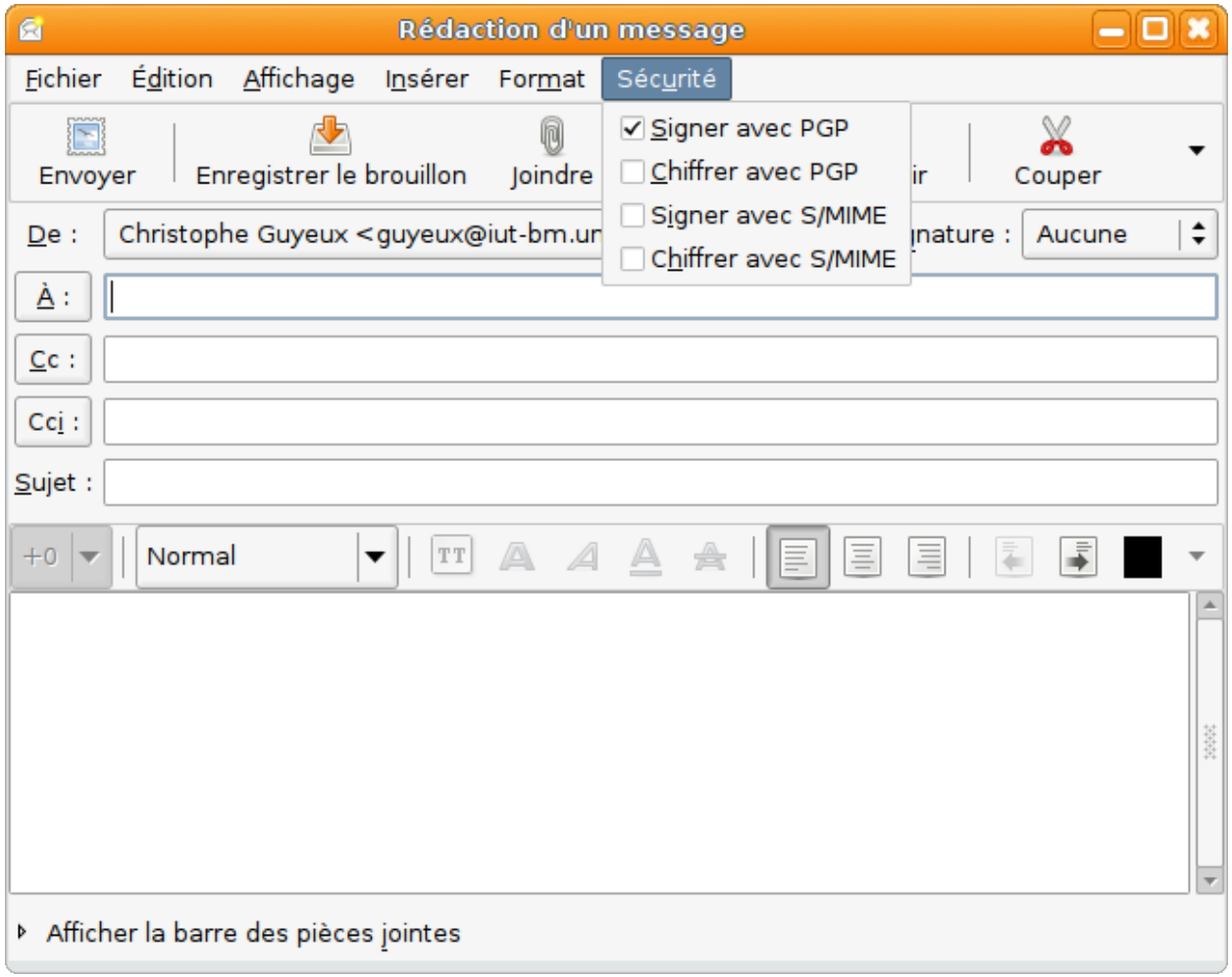
Présentation d'évolution

- On présente dans ce qui suit, à l'aide de captures d'écrans, différentes possibilités de la messagerie Evolutions, installée par défaut sous Ubuntu.
- On verra comment intégrer sa clé de chiffrement, et comment chiffrer ou signer un mail.
- On verra aussi la gestion des certificats.

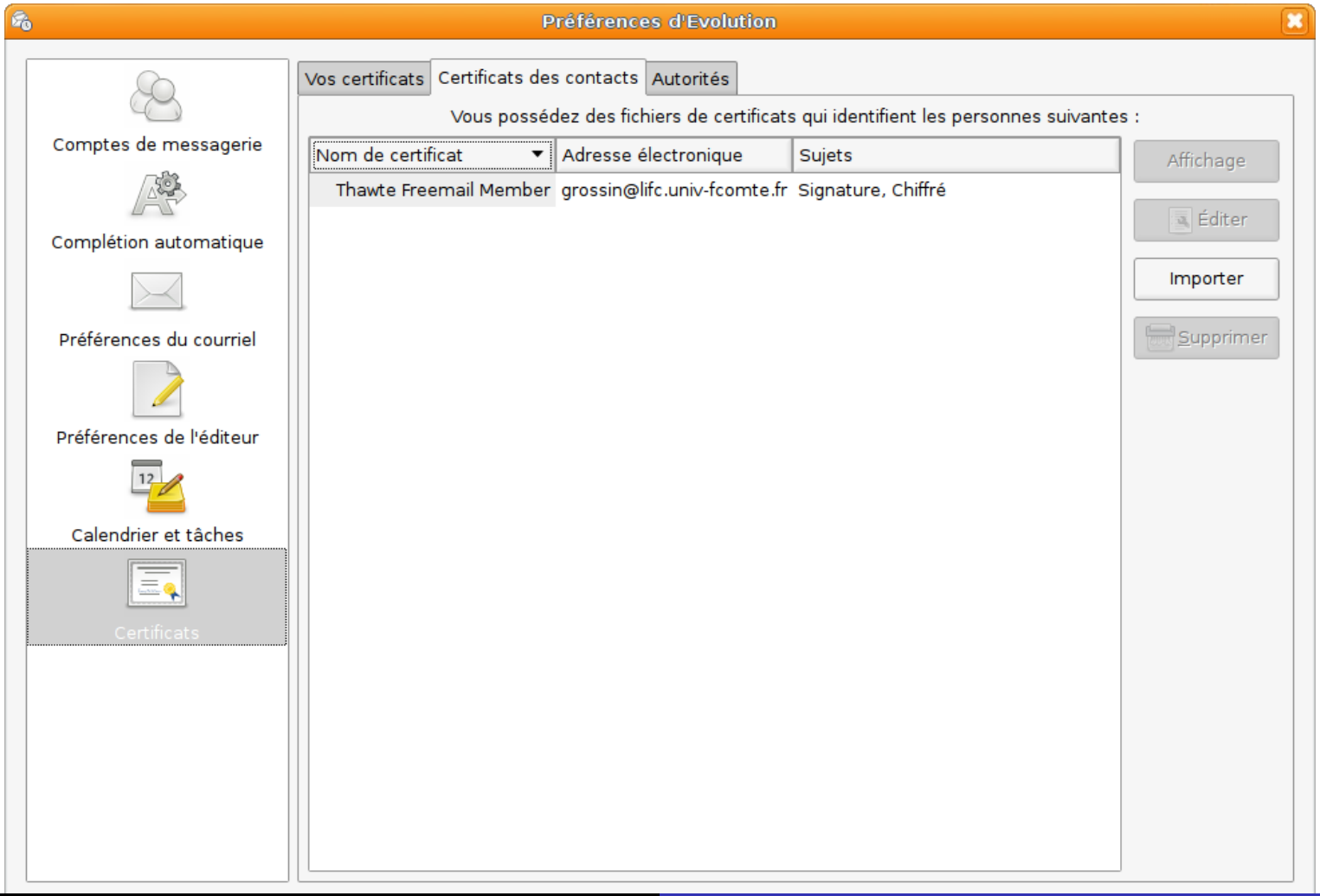
Configuration d'évolution



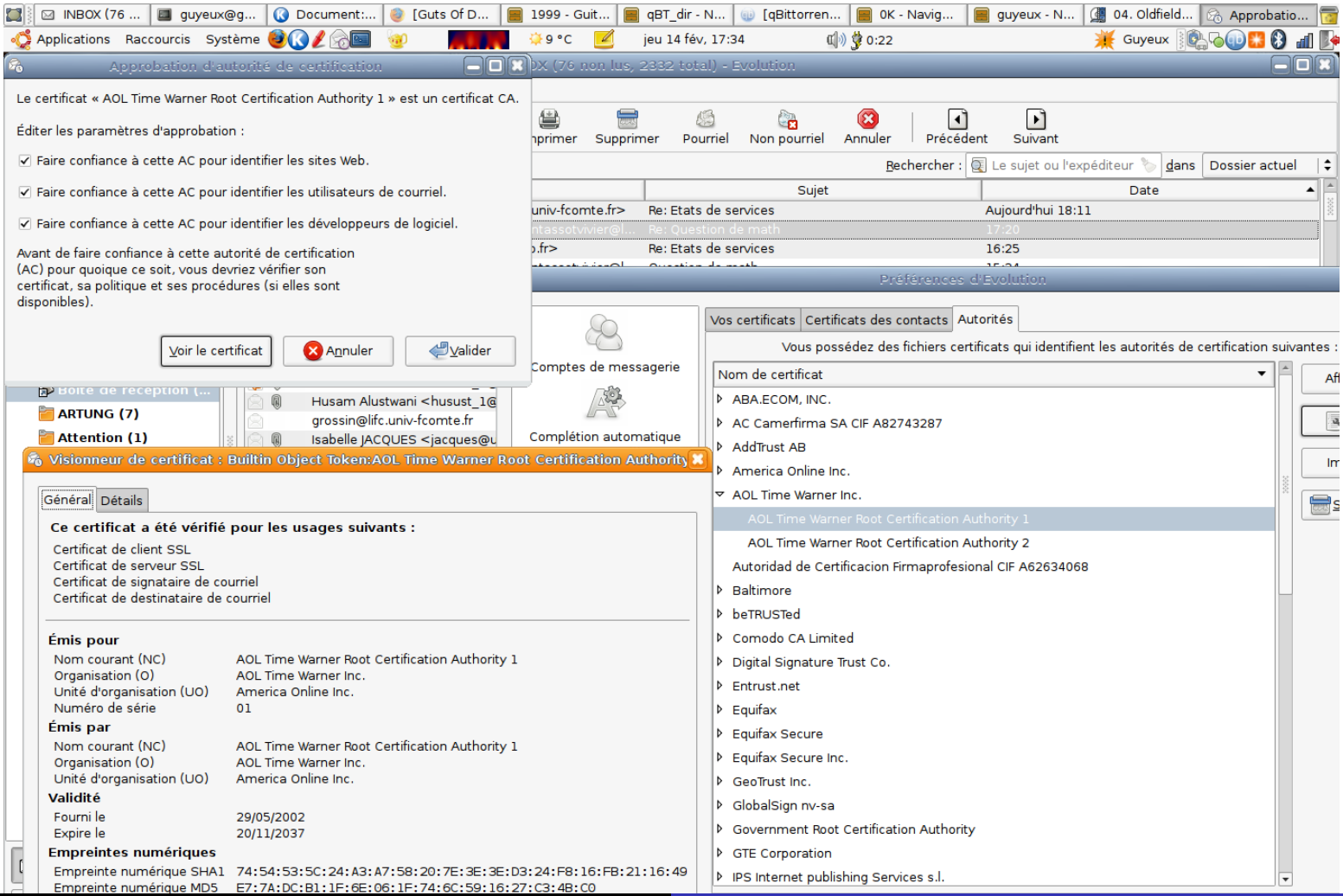
Envoi d'un mail chiffré ou signé



Evolution : les certificats



Evolution : les certificats



Des outils de sécurité

Des outils de sécurité

Shred : Détruire efficacement un fichier

Que se passe-t-il quand on supprime un fichier ?

Si vous supprimez un fichier, il n'est pas totalement supprimé :

Que se passe-t-il quand on supprime un fichier ?

Si vous supprimez un fichier, il n'est pas totalement supprimé :

- Si vous êtes sous Nautilus ou Konqueror, il est juste envoyé à la corbeille (/.Trash le plus souvent)

Que se passe-t-il quand on supprime un fichier ?

Si vous supprimez un fichier, il n'est pas totalement supprimé :

- Si vous êtes sous Nautilus ou Konqueror, il est juste envoyé à la corbeille (/.Trash le plus souvent)
- Si vous le supprimez sans passer par la corbeille (avec la commande rm par exemple), il n'est pas totalement supprimé.

Que se passe-t-il quand on supprime un fichier ?

Si vous supprimez un fichier, il n'est pas totalement supprimé :

- Si vous êtes sous Nautilus ou Konqueror, il est juste envoyé à la corbeille (/.Trash le plus souvent)
- Si vous le supprimez sans passer par la corbeille (avec la commande rm par exemple), il n'est pas totalement supprimé.
- L'espace disque correspondant est juste marqué comme étant « libre », mais il existe des logiciels permettant de retrouver ces données.

Le déchiquettage

- Pour supprimer efficacement un fichier, vous pouvez utiliser la commande shred (déchiquettage) :

Shell

```
shred -n 35 -z -u nomDuFichier
```

Le déchiquettage

- Pour supprimer efficacement un fichier, vous pouvez utiliser la commande shred (déchiquettage) :

Shell

```
shred -n 35 -z -u nomDuFichier
```

- Ceci a pour effet de :
  - remplacer 35 fois les données du fichier par des déchets
  - remplacer ces données par des zéros (-z) pour masquer le déchiquettage
  - tronquer et supprimer le fichier (-u)

Le déchiquettage

- Pour supprimer efficacement un fichier, vous pouvez utiliser la commande shred (déchiquettage) :

Shell

```
shred -n 35 -z -u nomDuFichier
```

- Ceci a pour effet de :
  - remplacer 35 fois les données du fichier par des déchets
  - remplacer ces données par des zéros (-z) pour masquer le déchiquettage
  - tronquer et supprimer le fichier (-u)
- Cette méthode est déjà plus efficace...mais il restera toujours des informations sur le fichier permettant de le retrouver (système de fichiers journalisé, *etc.*)

Des outils de sécurité

Des outils de sécurité

Tor

Présentation

- Le but de Tor est de se protéger de l'analyse de trafic.

Présentation

- Le but de Tor est de se protéger de l'analyse de trafic.
- C'est une forme de surveillance des réseaux qui menace l'anonymat et la confidentialité des personnes, les activités et les rapports confidentiels commerciaux.

Présentation

- Le but de Tor est de se protéger de l'analyse de trafic.
- C'est une forme de surveillance des réseaux qui menace l'anonymat et la confidentialité des personnes, les activités et les rapports confidentiels commerciaux.
- Avec Tor, les communications rebondissent à travers un réseau de serveurs distribués (nœuds), appelés onion routers.

Présentation

- Le but de Tor est de se protéger de l'analyse de trafic.
- C'est une forme de surveillance des réseaux qui menace l'anonymat et la confidentialité des personnes, les activités et les rapports confidentiels commerciaux.
- Avec Tor, les communications rebondissent à travers un réseau de serveurs distribués (nœuds), appelés onion routers.
- Ils vous protègent contre les sites web qui enregistrent les pages que vous visitez, contre les observateurs externes, et contre les onion routers eux-mêmes.

Présentation

- Tor réduit les risques d'analyses de trafic simples ou sophistiquées, en répartissant vos transactions entre plusieurs endroits de l'Internet.

Présentation

- Tor réduit les risques d'analyses de trafic simples ou sophistiquées, en répartissant vos transactions entre plusieurs endroits de l'Internet.
- On ne peut donc pas, en observant un seul point, vous associer à votre destinataire.

Présentation

- Tor réduit les risques d'analyses de trafic simples ou sophistiquées, en répartissant vos transactions entre plusieurs endroits de l'Internet.
- On ne peut donc pas, en observant un seul point, vous associer à votre destinataire.
- C'est comme utiliser un chemin tortueux et difficile à suivre pour semer un poursuivant (tout en effaçant de temps en temps ses traces).

Présentation

- Tor réduit les risques d'analyses de trafic simples ou sophistiquées, en répartissant vos transactions entre plusieurs endroits de l'Internet.
- On ne peut donc pas, en observant un seul point, vous associer à votre destinataire.
- C'est comme utiliser un chemin tortueux et difficile à suivre pour semer un poursuivant (tout en effaçant de temps en temps ses traces).
- Au lieu d'emprunter un itinéraire direct entre la source et la destination, les paquets de données suivent une trajectoire aléatoire à travers plusieurs serveurs qui font disparaître vos traces.

Présentation

- Personne ne peut donc déduire de l'observation d'un point unique, d'où viennent, ni où vont les données.

Présentation

- Personne ne peut donc déduire de l'observation d'un point unique, d'où viennent, ni où vont les données.

Shell

```
sudo apt-get install tor
```

Présentation

- Personne ne peut donc déduire de l'observation d'un point unique, d'où viennent, ni où vont les données.

Shell

```
sudo apt-get install tor
```

- Le paquet est configuré par défaut pour écouter sur l'interface de loopback (127.0.0.1) et sur le port 9050, tor lance un proxy supportant Socks4a et Socks5.

Présentation

- Personne ne peut donc déduire de l'observation d'un point unique, d'où viennent, ni où vont les données.

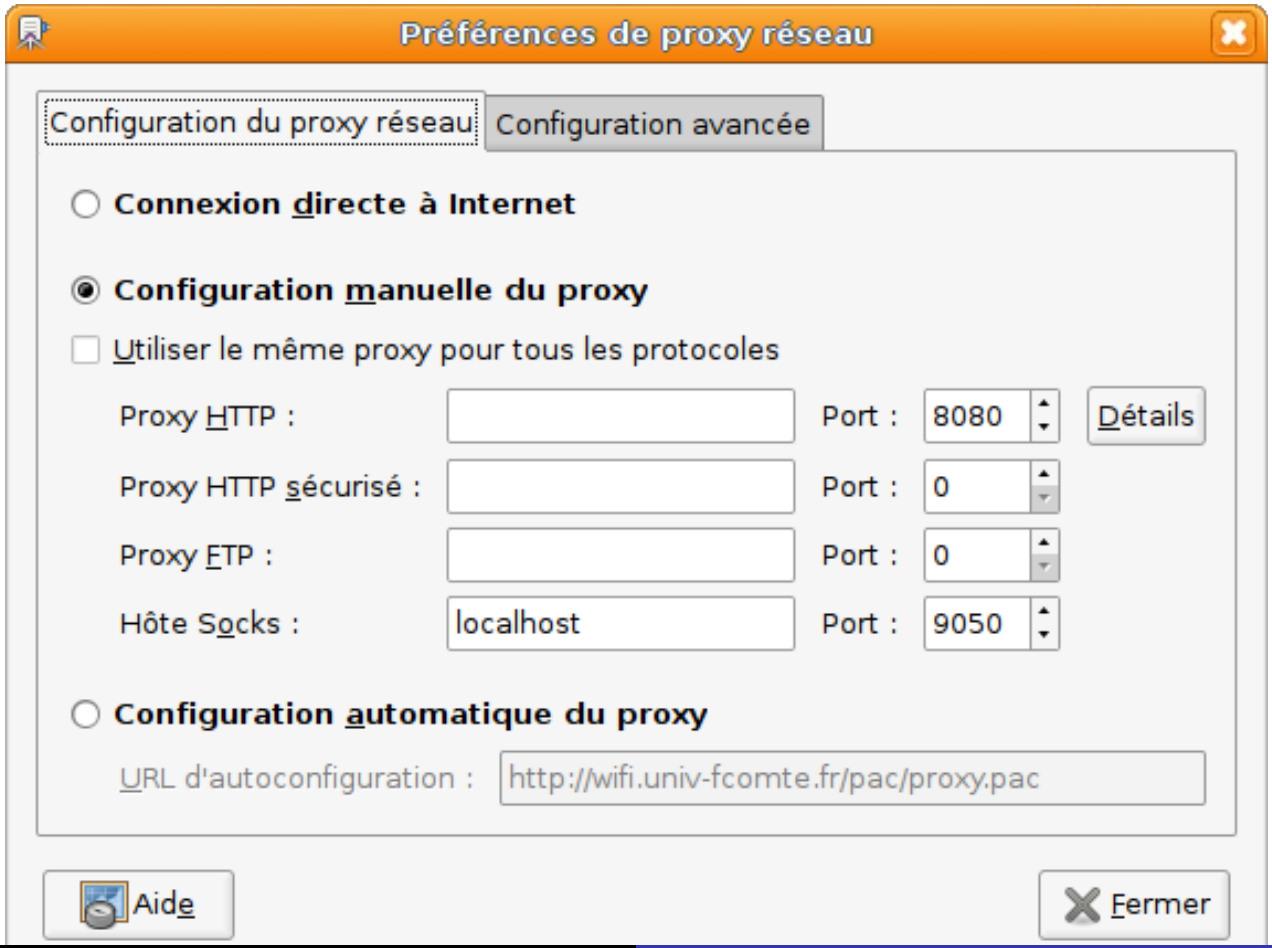
Shell

```
sudo apt-get install tor
```

- Le paquet est configuré par défaut pour écouter sur l'interface de loopback (127.0.0.1) et sur le port 9050, tor lance un proxy supportant Socks4a et Socks5.
- Il faut donc spécifier un proxy Socks utilisant l'adresse 127.0.0.1 (ou le nom d'hôte localhost) et le port 9050.

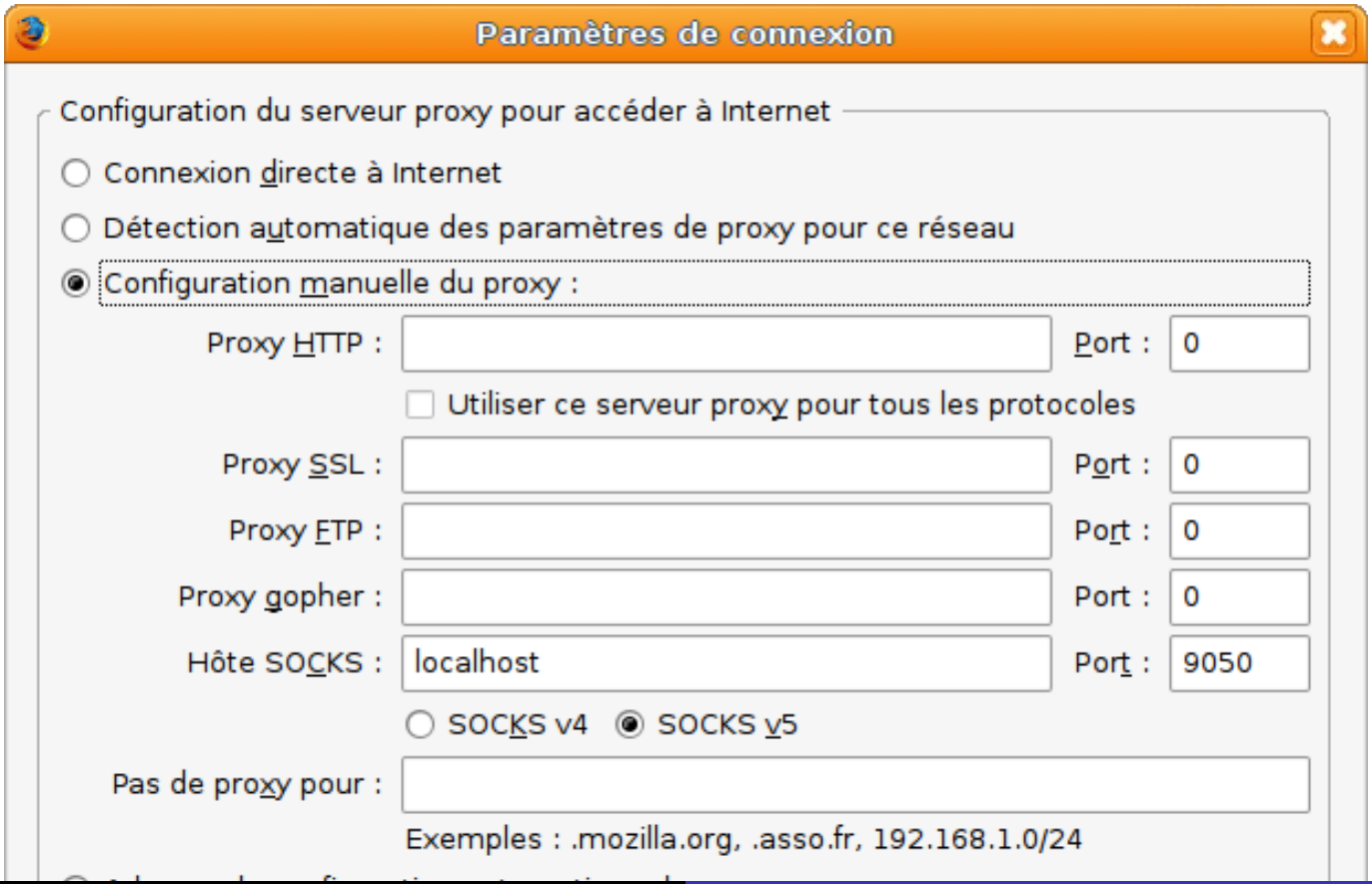
Proxy

Par exemple, dans Système -> Préférences -> Proxy réseau :

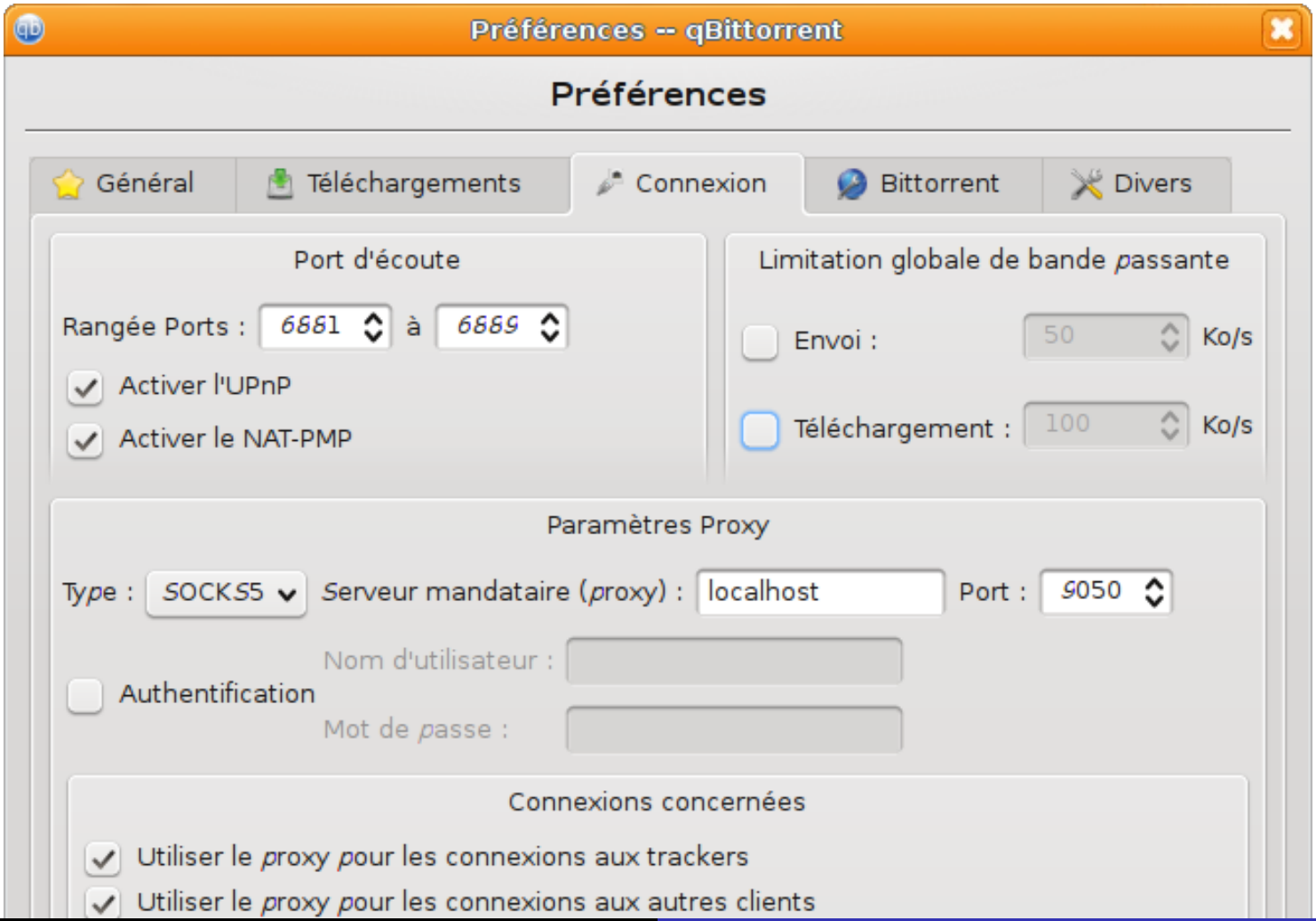


Proxy firefox

Pour firefox, dans Edition -> Préférences -> Avancé -> Réseau -> Paramètres :



Qbittorrent et Tor



Autour des mots de passe

Un bon mot de passe

Choix du mot de passe

- Un bon mot de passe contient au moins 8 caractères.

Choix du mot de passe

- Un bon mot de passe contient au moins 8 caractères.
- Il utilise le plus d'anarchie possible, c'est-à-dire majuscules, minuscules, symboles, chiffres et caractères spéciaux.

Choix du mot de passe

- Un bon mot de passe contient au moins 8 caractères.
- Il utilise le plus d'anarchie possible, c'est-à-dire majuscules, minuscules, symboles, chiffres et caractères spéciaux.
- Le mot ne doit pas apparaître dans un dictionnaire.

Choix du mot de passe

- Un bon mot de passe contient au moins 8 caractères.
- Il utilise le plus d'anarchie possible, c'est-à-dire majuscules, minuscules, symboles, chiffres et caractères spéciaux.
- Le mot ne doit pas apparaître dans un dictionnaire.
- Enfin, il ne doit pas être forgé à partir de données personnelles (date de naissance, nom du chien, *etc.*)

Recommandations

- Il est recommandé de changer de mot de passe régulièrement.

Recommandations

- Il est recommandé de changer de mot de passe régulièrement.
- De ne pas l'écrire autre part que dans son cerveau.

Recommandations

- Il est recommandé de changer de mot de passe régulièrement.
- De ne pas l'écrire autre part que dans son cerveau.
- De ne pas utiliser le même mot de passe pour s'authentifier en des lieux différents.

Astuce

- Pour se souvenir d'un mot de passe complexe on peut utiliser les premières lettres de chaque mot d'une poésie, d'un texte...

Astuce

- Pour se souvenir d'un mot de passe complexe on peut utiliser les premières lettres de chaque mot d'une poésie, d'un texte...
- Par exemple « Lsldvdl'a. » : « Les sanglots longs des violons de l'automne. »

Autour des mots de passe

John the Ripper

Avertissement

- Le but de ce qui suit est de vous convaincre que rien n'est plus facile que de casser un mot de passe mal réfléchi.

Avertissement

- Le but de ce qui suit est de vous convaincre que rien n'est plus facile que de casser un mot de passe mal réfléchi.
- Vous n'êtes pas sensé faire n'importe quoi avec...

Avertissement

- Le but de ce qui suit est de vous convaincre que rien n'est plus facile que de casser un mot de passe mal réfléchi.
- Vous n'êtes pas sensé faire n'importe quoi avec...
- Ce qui suit convient à une distribution Ubuntu, avec John the Ripper installé :

Shell

```
sudo apt-get install john
```

Un exemple

- Combien de temps résiste le mot de passe 654321 ?

Un exemple

- Combien de temps résiste le mot de passe 654321 ?
- On commence par créer un utilisateur de test, avec le mot de passe 654321 :

Shell

```
sudo adduser jambon
```

Un exemple

- Combien de temps résiste le mot de passe 654321 ?
- On commence par créer un utilisateur de test, avec le mot de passe 654321 :

Shell

```
sudo adduser jambon
```

- On récupère le fichier des utilisateurs, dont on change l'appartenance :

Shell

```
sudo cp /etc/shadow .
sudo chown christophe :christophe shadow
```

John en action

- Puis on envoie la sauce :

Shell

```
john shadow
```

John en action

- Puis on envoie la sauce :

Shell

```
john shadow
```

- et l'on obtient :

Shell

```
Loaded 3 passwords with 3 different salts (FreeBSD MD5
[32/32])
654321 (jambon)
guesses : 1 time : 0 :00 :00 :21 33% (2) c/s : 4000 trying : rose0
```

John en action

- Puis on envoie la sauce :

Shell

```
john shadow
```

- et l'on obtient :

Shell

```
Loaded 3 passwords with 3 different salts (FreeBSD MD5
[32/32])
654321 (jambon)
guesses : 1 time : 0 :00 :00 :21 33% (2) c/s : 4000 trying : rose0
```

- Il a donc fallu 21 centièmes de seconde pour craquer ce mot de passe.

Dictionnaire français

- John the Ripper utilise une liste de mots de passe (dans /usr/share/john/password.lst), liste valable pour les utilisateurs anglophones.

Dictionnaire français

- John the Ripper utilise une liste de mots de passe (dans /usr/share/john/password.lst), liste valable pour les utilisateurs anglophones.
- Pour installer un dictionnaire français :

Shell

```
sudo apt-get install wfrench
```

Dictionnaire français

- John the Ripper utilise une liste de mots de passe (dans /usr/share/john/password.lst), liste valable pour les utilisateurs anglophones.
- Pour installer un dictionnaire français :

Shell

```
sudo apt-get install wfrench
```

- Qui doit être convertis en UTF-8

Shell

```
iconv -f ISO-8859-15 -t utf-8 < /usr/share/dict/french >
/tmp/french.utf8.lst
```

Dictionnaire français

Enfin, on relance john, avec ce fichier pour dictionnaire :

Shell

```
john -wordfile :/tmp/french.utf8.lst -users :jambon shadow
```

Vérification régulière des mots de passe

- Pour lancer John the Ripper toutes les nuits, et être prévenu par mail en cas de succès...

Vérification régulière des mots de passe

- Pour lancer John the Ripper toutes les nuits, et être prévenu par mail en cas de succès...
- On active le cron, en éditant/etc/cron.d/john et en décommentant les deux lignes contenant /usr/share/john/cronjob (start et stop)

Vérification régulière des mots de passe

- Pour lancer John the Ripper toutes les nuits, et être prévenu par mail en cas de succès...
- On active le cron, en éditant/etc/cron.d/john et en décommentant les deux lignes contenant /usr/share/john/cronjob (start et stop)
- Par défaut, John travaillera de 1h à 7h.

Vérification régulière des mots de passe

- Pour lancer John the Ripper toutes les nuits, et être prévenu par mail en cas de succès...
- On active le cron, en éditant/etc/cron.d/john et en décommentant les deux lignes contenant /usr/share/john/cronjob (start et stop)
- Par défaut, John travaillera de 1h à 7h.
- Un mail sera alors envoyé à l'utilisateur craqué, que l'on peut modifier.

Autour des mots de passe

Autour des mots de passe

Firefox et ses mots de passe

Firefox et les mots de passes

- Les mots de passe, dans firefox, sont cryptés dans le fichier signons.txt du sous-répertoire .mozilla/firefox/XXX.default/ du répertoire personnel.

Firefox et les mots de passes

- Les mots de passe, dans firefox, sont cryptés dans le fichier signons.txt du sous-répertoire .mozilla/firefox/XXX.default/ du répertoire personnel.
- Le problème est qu'on peut les consulter en clair dans firefox.

Firefox et les mots de passes

- Les mots de passe, dans firefox, sont cryptés dans le fichier signons.txt du sous-répertoire .mozilla/firefox/XXX.default/ du répertoire personnel.
- Le problème est qu'on peut les consulter en clair dans firefox.
- Edition -> Préférences ->Sécurité, bouton *Afficher les mots de passe*, et le même bouton dans la fenêtre qui s'ouvre alors.

Firefox et les mots de passes

- Les mots de passe, dans firefox, sont cryptés dans le fichier signons.txt du sous-répertoire .mozilla/firefox/XXX.default/ du répertoire personnel.
- Le problème est qu'on peut les consulter en clair dans firefox.
- Edition -> Préférences ->Sécurité, bouton *Afficher les mots de passe*, et le même bouton dans la fenêtre qui s'ouvre alors.
- Pour éviter cela, on peut cocher la case : Utiliser un mot de passe principal.

Autour des mots de passe

Autour des mots de passe

Analyse statistique des mots de passe

Présentation

- Même si vous vous êtes fait subtiliser votre mot de passe, vous pouvez encore défendre vos données.

Présentation

- Même si vous vous êtes fait subtiliser votre mot de passe, vous pouvez encore défendre vos données.
- Cela peut se faire par la technique d'analyse statistique de l'entrée des passwords au clavier.

Présentation

- Même si vous vous êtes fait subtiliser votre mot de passe, vous pouvez encore défendre vos données.
- Cela peut se faire par la technique d'analyse statistique de l'entrée des passwords au clavier.
- Tout se passe à l'adresse : http ://www.ibm.com/developerworks/opensource/library/os-keys

Présentation

- Même si vous vous êtes fait subtiliser votre mot de passe, vous pouvez encore défendre vos données.
- Cela peut se faire par la technique d'analyse statistique de l'entrée des passwords au clavier.
- Tout se passe à l'adresse : http ://www.ibm.com/developerworks/opensource/library/os-keys
- Dans cet article, on vous détaille comment adapter le programme xev (X event viewer), qui s'occupe de la capture des évènements comme les frappes clavier.

L'analyse statistique

- Une fois cela fait, il vous suffira de passer ces évènements par l'intermédiaire d'un pipe, qui alimentera les scripts perl listés dans l'article pour analyser statistiquement la frappe des mots de passe.

L'analyse statistique

- Une fois cela fait, il vous suffira de passer ces évènements par l'intermédiaire d'un pipe, qui alimentera les scripts perl listés dans l'article pour analyser statistiquement la frappe des mots de passe.
- Ainsi vous aurez des chances de déceler l'imposteur se faisant passer pour votre user, et de lui interdire l'accès aux données.

L'analyse statistique

- Une fois cela fait, il vous suffira de passer ces évènements par l'intermédiaire d'un pipe, qui alimentera les scripts perl listés dans l'article pour analyser statistiquement la frappe des mots de passe.
- Ainsi vous aurez des chances de déceler l'imposteur se faisant passer pour votre user, et de lui interdire l'accès aux données.
- Les scripts permettent de vérifier le temps total d'entrée du password (qui pour un utilisateur légitime est remarquablement constant).

Analyse du temps de frappe

- On peut aussi analyser le temps entre chaque frappe clavier.

Analyse du temps de frappe

- On peut aussi analyser le temps entre chaque frappe clavier.
- Si par exemple l'utilisateur entre les lettres rapidement mais les chiffres lentement (il a un portable et doit appuyer sur shift à chaque fois)...

Analyse du temps de frappe

- On peut aussi analyser le temps entre chaque frappe clavier.
- Si par exemple l'utilisateur entre les lettres rapidement mais les chiffres lentement (il a un portable et doit appuyer sur shift à chaque fois)...
- ...Alors que le pirate entre les chiffres rapidement (il a un pavé numérique), alors l'analyse le détectera.

Introduction à la sécurité

Etre root sur une machine

Pourquoi protéger son BIOS ?

Si la configuration du BIOS d'un ordinateur n'est pas protégée par un mot de passe et si les partitions ne sont pas chiffrées, il est possible de :

1. Ouvrir l'utilitaire de configuration du BIOS au démarrage de l'ordinateur.

Pourquoi protéger son BIOS ?

Si la configuration du BIOS d'un ordinateur n'est pas protégée par un mot de passe et si les partitions ne sont pas chiffrées, il est possible de :

1. Ouvrir l'utilitaire de configuration du BIOS au démarrage de l'ordinateur.
2. Placer le lecteur CD-ROM en premier dans la séquence de démarrage (boot).

Pourquoi protéger son BIOS ?

Si la configuration du BIOS d'un ordinateur n'est pas protégée par un mot de passe et si les partitions ne sont pas chiffrées, il est possible de :

1. Ouvrir l'utilitaire de configuration du BIOS au démarrage de l'ordinateur.
2. Placer le lecteur CD-ROM en premier dans la séquence de démarrage (boot).
3. Placer un LiveCD dans le lecteur, avant de quitter en sauvegardant la configuration du démarrage.

Pourquoi protéger son BIOS ?

Si la configuration du BIOS d'un ordinateur n'est pas protégée par un mot de passe et si les partitions ne sont pas chiffrées, il est possible de :

1. Ouvrir l'utilitaire de configuration du BIOS au démarrage de l'ordinateur.
2. Placer le lecteur CD-ROM en premier dans la séquence de démarrage (boot).
3. Placer un LiveCD dans le lecteur, avant de quitter en sauvegardant la configuration du démarrage.
4. Démarrer sur le LiveCD et attendre.

Pourquoi protéger son BIOS ?

Si la configuration du BIOS d'un ordinateur n'est pas protégée par un mot de passe et si les partitions ne sont pas chiffrées, il est possible de :

1. Ouvrir l'utilitaire de configuration du BIOS au démarrage de l'ordinateur.
2. Placer le lecteur CD-ROM en premier dans la séquence de démarrage (boot).
3. Placer un LiveCD dans le lecteur, avant de quitter en sauvegardant la configuration du démarrage.
4. Démarrer sur le LiveCD et attendre.
5. Profiter de tous les droits root sur la machine.

Est-on protégé avec un mot de passe BIOS ?

- Le fait de choisir un mot de passe pour le BIOS peut aider à dissuader un intrus de s'approprier les droits root via LiveCD.

Est-on protégé avec un mot de passe BIOS ?

- Le fait de choisir un mot de passe pour le BIOS peut aider à dissuader un intrus de s'approprier les droits root via LiveCD.
- Mais il reste toujours possible de vider la mémoire du BIOS (et donc la protection par mot de passe) en ouvrant l'unité centrale.

Est-on protégé avec un mot de passe BIOS ?

- Le fait de choisir un mot de passe pour le BIOS peut aider à dissuader un intrus de s'approprier les droits root via LiveCD.
- Mais il reste toujours possible de vider la mémoire du BIOS (et donc la protection par mot de passe) en ouvrant l'unité centrale.
- Cela souligne un point important en matière de sécurité informatique : celle-ci est fortement compromise dès lors qu'un accès physique à la machine est permis.

Recovery mode

- Par défaut, le logiciel chargeur de système Grub inclut dans la liste des choix de système Ubuntu en Recovery mode.

Recovery mode

- Par défaut, le logiciel chargeur de système Grub inclut dans la liste des choix de système Ubuntu en Recovery mode.
- Il suffit de choisir cette option pour profiter des droits root sur la machine.

Recovery mode

- Par défaut, le logiciel chargeur de système Grub inclut dans la liste des choix de système Ubuntu en Recovery mode.
- Il suffit de choisir cette option pour profiter des droits root sur la machine.
- Et il n'y a pas de demande du mot de passe root !

Précautions

- On peut enlever le recovery mode des choix du grub.

Précautions

- On peut enlever le recovery mode des choix du grub.
- On doit aussi protéger le grub d'un mot de passe : en effet, au moment du choix du système, on peut éditer la ligne, et donc demander à être en mode recovery.

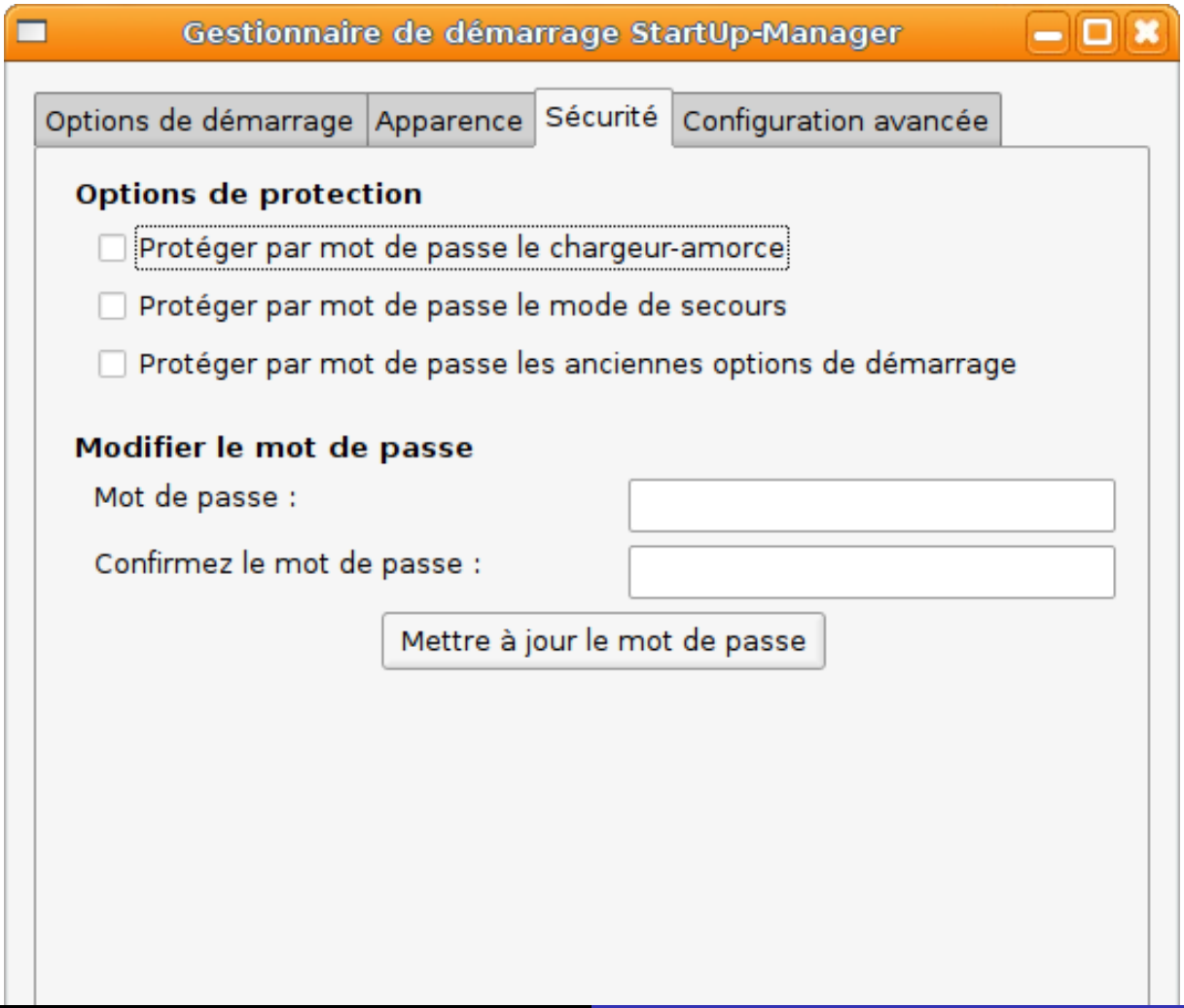
Précautions

- On peut enlever le recovery mode des choix du grub.
- On doit aussi protéger le grub d'un mot de passe : en effet, au moment du choix du système, on peut éditer la ligne, et donc demander à être en mode recovery.
- Tout cela se fait dans le fichier /boot/grub/menu.lst

Précautions

- On peut enlever le recovery mode des choix du grub.
- On doit aussi protéger le grub d'un mot de passe : en effet, au moment du choix du système, on peut éditer la ligne, et donc demander à être en mode recovery.
- Tout cela se fait dans le fichier /boot/grub/menu.lst
- Il existe aussi un logiciel graphique permettant cela : StartUp-Manager.

StartUp-Manager



Introduction à la sécurité

Les antivirus sous linux

Les risques d'infection

- Le temps moyen avant qu'un ordinateur sous Windows ne soit infecté est de 40 minutes (Connecté à l'Internet et avec une installation « Service Pack 2 » par défaut)

Les risques d'infection

- Le temps moyen avant qu'un ordinateur sous Windows ne soit infecté est de 40 minutes (Connecté à l'Internet et avec une installation « Service Pack 2 » par défaut)
- Il faut donc se dépêcher d'installer pare-feu et antivirus !

Les risques d'infection

- Le temps moyen avant qu'un ordinateur sous Windows ne soit infecté est de 40 minutes (Connecté à l'Internet et avec une installation « Service Pack 2 » par défaut)
- Il faut donc se dépêcher d'installer pare-feu et antivirus !
- Contrairement à cela, GNU/Linux n'a pratiquement pas de virus.

Linux plus sûr que Windows ?

- Bien sûr, un virus sous GNU/Linux n'est pas chose impossible.

Linux plus sûr que Windows ?

- Bien sûr, un virus sous GNU/Linux n'est pas chose impossible.
- Mais GNU/Linux est construit de telle sorte que cela ne peut arriver que très difficilement pour les raisons suivantes.

Linux plus sûr que Windows ?

- Bien sûr, un virus sous GNU/Linux n'est pas chose impossible.
- Mais GNU/Linux est construit de telle sorte que cela ne peut arriver que très difficilement pour les raisons suivantes.
- La plupart des gens utilisent Windows, et les pirates cherchent à faire le plus de dommages possibles.

Linux plus sûr que Windows ?

- Bien sûr, un virus sous GNU/Linux n'est pas chose impossible.
- Mais GNU/Linux est construit de telle sorte que cela ne peut arriver que très difficilement pour les raisons suivantes.
- La plupart des gens utilisent Windows, et les pirates cherchent à faire le plus de dommages possibles.
- Cela n'est pas l'unique raison, car par exemple le serveur web Apache possède la plus grande part de marché — contre le serveur ISS de Microsoft...

Linux plus sûr que Windows ?

- Bien sûr, un virus sous GNU/Linux n'est pas chose impossible.
- Mais GNU/Linux est construit de telle sorte que cela ne peut arriver que très difficilement pour les raisons suivantes.
- La plupart des gens utilisent Windows, et les pirates cherchent à faire le plus de dommages possibles.
- Cela n'est pas l'unique raison, car par exemple le serveur web Apache possède la plus grande part de marché — contre le serveur ISS de Microsoft...
- Mais il a beaucoup moins de trous de sécurité et subit beaucoup moins d'attaques que celui de Microsoft.

L'avantage du code disponible

- De plus, les Logiciels Libres permettent à n'importe qui de vérifier leur code.

L'avantage du code disponible

- De plus, les Logiciels Libres permettent à n'importe qui de vérifier leur code.
- N'importe quel programmeur sur la Terre peut télécharger le code, jeter un coup d'œil, et voir si des failles de sécurité peuvent exister.

L'avantage du code disponible

- De plus, les Logiciels Libres permettent à n'importe qui de vérifier leur code.
- N'importe quel programmeur sur la Terre peut télécharger le code, jeter un coup d'œil, et voir si des failles de sécurité peuvent exister.
- En revanche, les seules personnes autorisées à voir le code source de Windows sont celles qui travaillent chez Microsoft.

L'avantage du code disponible

- De plus, les Logiciels Libres permettent à n'importe qui de vérifier leur code.
- N'importe quel programmeur sur la Terre peut télécharger le code, jeter un coup d'œil, et voir si des failles de sécurité peuvent exister.
- En revanche, les seules personnes autorisées à voir le code source de Windows sont celles qui travaillent chez Microsoft.
- Cela représente des centaines de milliers de gens contre quelques milliers.

Importance des failles

- Mais à vrai dire, le problème n'est pas vraiment combien de failles un système possède, comparé aux autres.

Importance des failles

- Mais à vrai dire, le problème n'est pas vraiment combien de failles un système possède, comparé aux autres.
- S'il y a beaucoup de failles, mais :
  - que personne ne les a encore découvertes — y compris les pirates,
  - ou qu'elles sont mineures — c'est à dire qu'elles ne compromettent pas l'intégrité d'une part importante du système,

  les pirates ne seront pas capables de faire beaucoup de dégâts.

Importance des failles

- Mais à vrai dire, le problème n'est pas vraiment combien de failles un système possède, comparé aux autres.
- S'il y a beaucoup de failles, mais :
  - que personne ne les a encore découvertes — y compris les pirates,
  - ou qu'elles sont mineures — c'est à dire qu'elles ne compromettent pas l'intégrité d'une part importante du système,

  les pirates ne seront pas capables de faire beaucoup de dégâts.
- La question est surtout combien de temps s'écoulera entre la découverte d'une faille de sécurité et la publication d'un correctif.

Exemple d'une faille réelle sous Ubuntu

- Sur une installation toute fraîche de Breezy (ie avant d'avoir effectué les mises à jour de sécurité) taper en ligne de commande :

g

```
rep -A 1 'password$' /var/log/installer/cdebconf/questions.dat
```

Exemple d'une faille réelle sous Ubuntu

- Sur une installation toute fraîche de Breezy (ie avant d'avoir effectué les mises à jour de sécurité) taper en ligne de commande :

g

```
rep -A 1 'password$' /var/log/installer/cdebconf/questions.dat
```

- ...pour obtenir le mot de passe rentré lors de l'installation. Et ce, en clair et sans avoir besoin de superprivilèges.

Exemple d'une faille réelle sous Ubuntu

- Sur une installation toute fraîche de Breezy (ie avant d'avoir effectué les mises à jour de sécurité) taper en ligne de commande :

g

```
rep -A 1 'password$' /var/log/installer/cdebconf/questions.dat
```

- ...pour obtenir le mot de passe rentré lors de l'installation. Et ce, en clair et sans avoir besoin de superprivilèges.
- Relancer cette commande après avoir effectué les mises à jour de sécurité : ça ne fonctionne plus.

Correction d'une faille

- Si une faille est découverte dans un Logiciel Libre, n'importe qui dans la communauté « open source » peut venir voir et donner un coup de main.

Correction d'une faille

- Si une faille est découverte dans un Logiciel Libre, n'importe qui dans la communauté « open source » peut venir voir et donner un coup de main.
- La solution, et la mise à jour, apparaissent en général en quelques jours, voire en quelques heures.

Correction d'une faille

- Si une faille est découverte dans un Logiciel Libre, n'importe qui dans la communauté « open source » peut venir voir et donner un coup de main.
- La solution, et la mise à jour, apparaissent en général en quelques jours, voire en quelques heures.
- Une fois la mise à jour effectuée, vous êtes protégé (à moins que vous ne fassiez jamais vos mises à jours).

Correction d'une faille

- Si une faille est découverte dans un Logiciel Libre, n'importe qui dans la communauté « open source » peut venir voir et donner un coup de main.
- La solution, et la mise à jour, apparaissent en général en quelques jours, voire en quelques heures.
- Une fois la mise à jour effectuée, vous êtes protégé (à moins que vous ne fassiez jamais vos mises à jours).
- Microsoft ne dispose pas d'autant de « main-d'œuvre », et publie généralement un correctif environ un mois après la découverte de la faille.

Correction d'une faille

- Si une faille est découverte dans un Logiciel Libre, n'importe qui dans la communauté « open source » peut venir voir et donner un coup de main.
- La solution, et la mise à jour, apparaissent en général en quelques jours, voire en quelques heures.
- Une fois la mise à jour effectuée, vous êtes protégé (à moins que vous ne fassiez jamais vos mises à jours).
- Microsoft ne dispose pas d'autant de « main-d'œuvre », et publie généralement un correctif environ un mois après la découverte de la faille.
- Or, cette faille est parfois rendue publique : c'est plus qu'il n'en faut aux pirates pour faire ce qu'ils veulent avec votre ordinateur

A propos des autorisations

- Enfin, GNU/Linux possède une gestion intelligente des autorisations.

A propos des autorisations

- Enfin, GNU/Linux possède une gestion intelligente des autorisations.
- Sous Windows, vous – et par conséquent n'importe quel programme que vous installez – avez en général le droit de faire à peu près ce que vous voulez sur le système.

A propos des autorisations

- Enfin, GNU/Linux possède une gestion intelligente des autorisations.
- Sous Windows, vous – et par conséquent n'importe quel programme que vous installez – avez en général le droit de faire à peu près ce que vous voulez sur le système.
- Vous pouvez par exemple aller jeter un coup d'œil dans le dossier système et jeter ce que vous voulez dans la corbeille : Windows ne dira rien.

A propos des autorisations

- Enfin, GNU/Linux possède une gestion intelligente des autorisations.
- Sous Windows, vous – et par conséquent n'importe quel programme que vous installez – avez en général le droit de faire à peu près ce que vous voulez sur le système.
- Vous pouvez par exemple aller jeter un coup d'œil dans le dossier système et jeter ce que vous voulez dans la corbeille : Windows ne dira rien.
- Pensez que si vous pouvez détruire ces fichiers système, les autres programmes le peuvent aussi.

Linux et les droits utilisateurs

- GNU/Linux ne permet pas cela.

Linux et les droits utilisateurs

- GNU/Linux ne permet pas cela.
- Chaque fois que vous demandez à effectuer une opération en rapport avec le système, on vous demande un mot de passe d'administrateur.

Linux et les droits utilisateurs

- GNU/Linux ne permet pas cela.
- Chaque fois que vous demandez à effectuer une opération en rapport avec le système, on vous demande un mot de passe d'administrateur.
- Et si vous n'êtes pas administrateur sur ce système, vous n'en aurez simplement pas le droit.

Linux et les droits utilisateurs

- GNU/Linux ne permet pas cela.
- Chaque fois que vous demandez à effectuer une opération en rapport avec le système, on vous demande un mot de passe d'administrateur.
- Et si vous n'êtes pas administrateur sur ce système, vous n'en aurez simplement pas le droit.
- Les virus ne peuvent pas se balader tranquillement et effacer ou modifier ce qu'ils veulent dans le système : ils n'en ont pas l'autorisation, puisque vous-même, vous ne l'avez pas !

Conclusion partielle : pas d'antivirus nécessaire sous linux

- Globalement, l'utilisation d'un antivirus n'est pas nécesaire du moment que vous faites régulièrement les mises à jour.

Conclusion partielle : pas d'antivirus nécessaire sous linux

- Globalement, l'utilisation d'un antivirus n'est pas nécesaire du moment que vous faites régulièrement les mises à jour.
- Si vous n'êtes pas convaincu, vous pouvez toujours alourdir votre machine en installant un antivirus comme le paquet « ClamAV 34 ».

Conclusion partielle : pas d'antivirus nécessaire sous linux

- Globalement, l'utilisation d'un antivirus n'est pas nécesaire du moment que vous faites régulièrement les mises à jour.
- Si vous n'êtes pas convaincu, vous pouvez toujours alourdir votre machine en installant un antivirus comme le paquet « ClamAV 34 ».
- Et, après tout, si vous ne risquez pas grand chose, vos correspondants peuvent cependant être infectés de votre faute (transmission d'un mail infecté, *etc.*)

Se protéger, pour protéger les utilisateurs de Windows

- Clam AntiVirus (ClamAV), est un logiciel antivirus très utilisé sous UNIX.

Se protéger, pour protéger les utilisateurs de Windows

- Clam AntiVirus (ClamAV), est un logiciel antivirus très utilisé sous UNIX.
- Il est généralement utilisé avec les serveurs de courriels pour filtrer les courriers comportant des virus.

Se protéger, pour protéger les utilisateurs de Windows

- Clam AntiVirus (ClamAV), est un logiciel antivirus très utilisé sous UNIX.
- Il est généralement utilisé avec les serveurs de courriels pour filtrer les courriers comportant des virus.
- Les virus ciblés sont très majoritairement des virus s'attaquant au système d'exploitation Microsoft Windows et non pas aux systèmes sur lesquels ClamAV s'installe, peu menacés par les virus.

ClamAv

- En configurant ClamAV, le logiciel effectue la mise à jour automatique de la liste des virus ; celle-ci est directement téléchargé sur Internet.

ClamAv

- En configurant ClamAV, le logiciel effectue la mise à jour automatique de la liste des virus ; celle-ci est directement téléchargé sur Internet.
- ClamAV a la chance d'être libre et évolue très rapidement, notamment grâce aux utilisateurs qui envoient régulièrement aux développeurs de nouveaux virus pour les intégrer à la liste de souches connues.

ClamAv

- En configurant ClamAV, le logiciel effectue la mise à jour automatique de la liste des virus ; celle-ci est directement téléchargé sur Internet.
- ClamAV a la chance d'être libre et évolue très rapidement, notamment grâce aux utilisateurs qui envoient régulièrement aux développeurs de nouveaux virus pour les intégrer à la liste de souches connues.
- Début février 2008, il dépasse la barre des 200 000 logiciels malveillants reconnus.

Introduction à la sécurité

Firewall sous linux

Rappels sur les pare-feux

- Un pare-feu est un programme exécuté généralement en arrière-plan, en tant que service.

Rappels sur les pare-feux

- Un pare-feu est un programme exécuté généralement en arrière-plan, en tant que service.
- C'est une sécurité supplémentaire.

Rappels sur les pare-feux

- Un pare-feu est un programme exécuté généralement en arrière-plan, en tant que service.
- C'est une sécurité supplémentaire.
- Tout ordinateur relié à un réseau possède des entrées et des sorties qui servent à faire transiter les données.

Rappels sur les pare-feux

- Un pare-feu est un programme exécuté généralement en arrière-plan, en tant que service.
- C'est une sécurité supplémentaire.
- Tout ordinateur relié à un réseau possède des entrées et des sorties qui servent à faire transiter les données.
- Le pare-feu surveille ces « portes ».

Rappels sur les pare-feux

- Un pare-feu est un programme exécuté généralement en arrière-plan, en tant que service.
- C'est une sécurité supplémentaire.
- Tout ordinateur relié à un réseau possède des entrées et des sorties qui servent à faire transiter les données.
- Le pare-feu surveille ces « portes ».
- Il empêche les « visites » non sollicitées, tout en laissant passer ce que vous lui aurez dit de laisser passer.

Pare-feu sous linux

- Linux utilise un firewall par défaut nommé iptable, qui est installé automatiquement.

Pare-feu sous linux

- Linux utilise un firewall par défaut nommé iptable, qui est installé automatiquement.
- Sa politique par défaut est très stricte : toute communication initiée de l'extérieur vers les ports – portes communiquant avec l'extérieur – est interdite.

Pare-feu sous linux

- Linux utilise un firewall par défaut nommé iptable, qui est installé automatiquement.
- Sa politique par défaut est très stricte : toute communication initiée de l'extérieur vers les ports – portes communiquant avec l'extérieur – est interdite.
- Une interface graphique existe et se nomme FireStarter.

Introduction à la sécurité

Les rootkits

Qu'est-ce qu'un rootkit ?

- Un rootkit s'utilise après une intrusion et l'installation d'une porte dérobée afin de camoufler tous les changements effectués lors de l'intrusion.

Qu'est-ce qu'un rootkit ?

- Un rootkit s'utilise après une intrusion et l'installation d'une porte dérobée afin de camoufler tous les changements effectués lors de l'intrusion.
- Ainsi l'on peut préserver l'accès à la machine un maximum de temps.

Qu'est-ce qu'un rootkit ?

- Un rootkit s'utilise après une intrusion et l'installation d'une porte dérobée afin de camoufler tous les changements effectués lors de l'intrusion.
- Ainsi l'on peut préserver l'accès à la machine un maximum de temps.
- En effet les rootkits sont difficilement détectables et seule une analyse approfondie peut en révéler la présence.

Qu'est-ce qu'un rootkit ?

- Ces portes dérobées permettent au pirate de s'introduire à nouveau au cœur de la machine.

Qu'est-ce qu'un rootkit ?

- Ces portes dérobées permettent au pirate de s'introduire à nouveau au cœur de la machine.
- Et cela, sans pour autant exploiter une nouvelle fois la faille avec laquelle il a pu obtenir l'accès frauduleux initial, qui serait tôt ou tard comblée.

Qu'est-ce qu'un rootkit ?

- Ces portes dérobées permettent au pirate de s'introduire à nouveau au cœur de la machine.
- Et cela, sans pour autant exploiter une nouvelle fois la faille avec laquelle il a pu obtenir l'accès frauduleux initial, qui serait tôt ou tard comblée.
- Les « rootkit » opèrent une suite de modifications, notamment au niveau des commandes système, voire du noyau (kernel).

Comment ça marche

- L'installation d'un « rootkit » nécessite des droits administrateur sur la machine, notamment à cause des modifications profondes du système qu'il engendre.

Comment ça marche

- L'installation d'un « rootkit » nécessite des droits administrateur sur la machine, notamment à cause des modifications profondes du système qu'il engendre.
- Cela signifie que le pirate doit initialement disposer d'un accès frauduleux, avec les droits du « root » sous Linux par exemple, afin de mettre en place son « rootkit ».

Comment s'en prémunir

- Le « rootkit » n'a de raison d'être que si une faille est présente, si les conditions sont réunies pour que son exploitation soit réussie et si elle permet un accès avec les droits administrateur.

Comment s'en prémunir

- Le « rootkit » n'a de raison d'être que si une faille est présente, si les conditions sont réunies pour que son exploitation soit réussie et si elle permet un accès avec les droits administrateur.
- Le meilleur moyen de se protéger des rootkit est de se prémunir contre les failles.

Comment s'en prémunir

- Le « rootkit » n'a de raison d'être que si une faille est présente, si les conditions sont réunies pour que son exploitation soit réussie et si elle permet un accès avec les droits administrateur.
- Le meilleur moyen de se protéger des rootkit est de se prémunir contre les failles.
- Des applications existent cependant, qui permettent de tester son système, pour voir s'il n'est pas infecté.

En pratique, sous Ubuntu

- Pour Ubuntu, deux logiciel de détection de rootkits existent : rkhunter et chkrootkit.

En pratique, sous Ubuntu

- Pour Ubuntu, deux logiciel de détection de rootkits existent : rkhunter et chkrootkit.
- Si vous voulez les installer tapez cette commande dans une console :

Shell

```
sudo apt-get install rkhunter chkrootkit
```

En pratique, sous Ubuntu

- Pour Ubuntu, deux logiciel de détection de rootkits existent : rkhunter et chkrootkit.
- Si vous voulez les installer tapez cette commande dans une console :

Shell

```
sudo apt-get install rkhunter chkrootkit
```

- Pour scanner votre système :

Shell

```
sudo rkhunter -c
sudo chkrootkit
```

Est-ce si simple de se prémunir ?

- Les intrusions fréquentes sont effectuées par des script-kiddies : des pirates amateurs

Est-ce si simple de se prémunir ?

- Les intrusions fréquentes sont effectuées par des script-kiddies : des pirates amateurs
- Ils utilisent des failles de sécurité connues et des outils les exploitant créés par d'autres.

Est-ce si simple de se prémunir ?

- Les intrusions fréquentes sont effectuées par des script-kiddies : des pirates amateurs
- Ils utilisent des failles de sécurité connues et des outils les exploitant créés par d'autres.
- Fondamentalement, 95% des attaques sont toujours faites avec une poignée de rootkits connus.

Est-ce si simple de se prémunir ?

- Les intrusions fréquentes sont effectuées par des script-kiddies : des pirates amateurs
- Ils utilisent des failles de sécurité connues et des outils les exploitant créés par d'autres.
- Fondamentalement, 95% des attaques sont toujours faites avec une poignée de rootkits connus.
- Dès lors, si vous avez été piraté par un amateur, cela devrait être détecté avec les quelques outils présentés ici.