

guide d'autodéfense numérique

tome 1
hors connexions



troisième édition

été 2014

ouvrage collectif

Guide d'autodéfense numérique

Tome 1 : Hors connexions
troisième édition

Ouvrage collectif
guide@boum.org

Empreinte OpenPGP :
D487 4FA4 F6B6 88DC 0913
C9FD 326F 9F67 250B 0939

été 2014



Copyleft : cette œuvre est libre, vous pouvez la copier, la diffuser et la modifier selon les termes de la *Licence Art Libre* — <http://www.artlibre.org/>

Préface

Les revers de la mémoire numérique

De nos jours, les ordinateurs, Internet et le téléphone portable tendent à prendre de plus en plus de place dans nos vies. Le numérique semble souvent très pratique : c'est rapide, on peut parler avec plein de gens très loin, on peut avoir toute son histoire en photos, on peut écrire facilement des textes bien mis en page... mais ça n'a pas que des avantages ; ou en tout cas, ça n'en a pas seulement pour nous, mais aussi pour d'autres personnes qu'on n'a pas forcément envie d'aider.

Il est en effet bien plus facile d'écouter discrètement des conversations par le biais des téléphones portables que dans une rue bruyante, ou de trouver les informations que l'on veut sur un disque dur, plutôt que dans une étagère débordante de papiers.

De plus, énormément de nos informations personnelles finissent par se retrouver publiées quelque part, que ce soit par nous-mêmes ou par d'autres personnes, que ce soit parce qu'on nous y incite — c'est un peu le fond de commerce du *web 2.0*, parce que les technologies laissent des traces, ou simplement parce qu'on ne fait pas attention.

Rien à cacher ?

« *Mais faut pas être parano : je n'ai rien à cacher !* » pourrait-on répondre au constat précédent...

Deux exemples tout bêtes tendent pourtant à montrer le contraire : personne ne souhaite voir ses codes secrets de carte bleue ou de compte *eBay* tomber entre n'importe quelles mains ; et personne non plus n'aimerait voir quelqu'un qui ne lui veut pas du bien débarquer chez lui parce que son adresse a été publiée sur Internet malgré lui...

Mais au-delà de ces bêtes questions de défense de la propriété privée, la confidentialité des données devrait être *en soi* un enjeu.

Tout d'abord, parce que ce n'est pas nous qui jugeons de ce qu'il est autorisé ou non de faire avec un ordinateur. Des personnes arrêtées pour des activités numériques qui ne plaisaient pas à leur gouvernement croupissent en prison dans tous les pays du monde — pas seulement en Chine ou en Iran.

De plus, ce qui est autorisé aujourd'hui, comment savoir ce qu'il en sera demain ? Les gouvernements changent, les lois et les situations aussi. Si on n'a pas à cacher aujourd'hui, par exemple, la fréquentation régulière d'un site web militant, comment savoir ce qu'il en sera si celui-ci se trouve lié à un processus de répression ? Les traces *auront été laissées* sur l'ordinateur... et pourraient être employées comme élément à charge.

Enfin et surtout, à l'époque des sociétés de contrôles de plus en plus paranoïaques, de plus en plus résolues à traquer la subversion et à voir derrière chaque citoyen un

terroriste en puissance qu'il faut surveiller en conséquence, se cacher devient en soi un enjeu *politique*, ne serait-ce que pour mettre des bâtons dans les roues de ceux qui nous voudraient transparents et repérables en permanence.

Quoi qu'il en soit, beaucoup de gens, que ce soient les gouvernants, les employeurs, les publicitaires ou les flics¹, ont un intérêt à obtenir l'accès à nos données, surtout au vu de la place qu'a pris l'information dans l'économie et la politique mondiales.

Tout ça peut amener à se dire que nous n'avons pas envie d'être contrôlables par quelque « Big Brother » que ce soit. Qu'il existe déjà ou que l'on anticipe son émergence, le mieux est sans doute de faire en sorte qu'il ne puisse pas utiliser, contre nous, tous ces merveilleux outils que nous offrent — ou que lui offrent — les technologies modernes.

Aussi, *ayons tous quelque chose à cacher, ne serait-ce que pour brouiller les pistes !*

Comprendre pour pouvoir choisir

Ce guide se veut une tentative de décrire dans des termes compréhensibles l'intimité (ou plutôt son absence) dans le monde numérique ; une mise au point sur certaines idées reçues, afin de mieux comprendre à quoi on s'expose dans tel ou tel usage de tel ou tel outil. Afin, aussi, de pouvoir faire le tri parmi les « solutions », toutes plus ou moins dangereuses si l'on ne se rend pas compte de ce contre quoi elles ne protègent pas.

À la lecture de ces quelques pages, on pourra avoir le sentiment que rien n'est vraiment sûr avec un ordinateur ; et bien, c'est vrai. Et c'est faux. Il y a des outils et des usages appropriés. Et souvent la question n'est finalement pas tant « doit-on utiliser ou pas ces technologies ? », mais plutôt « quand et comment les utiliser (ou pas) ? »

Prendre le temps de comprendre

Des logiciels simples d'utilisation meurent d'envie de se substituer à nos cerveaux... s'ils nous permettent un usage facile de l'informatique, ils nous enlèvent aussi prise sur les bouts de vie qu'on leur confie.

Avec l'accélération des ordinateurs, de nos connexions à Internet, est arrivé le règne de l'instantanéité. Grâce au téléphone portable et au Wi-Fi, faire le geste de décrocher un téléphone ou de brancher un câble réseau à son ordinateur pour communiquer est déjà désuet.

Être patient, prendre le temps d'apprendre ou de réfléchir deviendrait superflu : on veut tout, tout de suite, on veut *la* solution. Mais cela implique de confier de nombreuses décisions à de distants experts que l'on croit sur parole. Ce guide a pour but de proposer d'autres solutions, qui nécessitent de prendre le temps de les comprendre et de les appliquer.

Adapter ses pratiques à l'usage qu'on a du monde numérique est donc nécessaire dès lors qu'on veut, ou qu'on doit, apporter une certaine attention à son impact. Mais la traversée n'a que peu de sens en solitaire. Nous vous enjoignons donc à construire autour de vous votre radeau numérique, à sauter joyeusement à bord, sans oublier d'emmener ce guide et quelques fusées de détresse pour envoyer vos remarques à guide@boum.org (avec les précautions nécessaires).

Un « guide »

Ce guide est une tentative de rassembler ce que nous avons pu apprendre au cours de nos années de pratiques, d'erreurs, de réflexions et de discussions pour le partager.

1. On utilise ici le terme « flics » tel qu'il est défini dans l'introduction de *Face à la police / Face à la justice* [<http://guidejuridique.net/>].

Non seulement les technologies évoluent très vite, mais nous avons pu commettre des erreurs ou écrire des contre-vérités dans ces pages. Nous tenterons donc de tenir ces notes à jour à l'adresse : <https://guide.boum.org/>

Afin de rendre le tout plus digeste, nous avons divisé tout ce que nous souhaitons raconter en plusieurs tomes. Qu'on se trouve avec uniquement un ordinateur, que ce dernier soit connecté à un réseau ou qu'on soit chez soi ou au téléphone, cela représente des contextes différents, donc des menaces, des envies et des réponses différentes elles aussi.

Préface à la troisième édition

Il y a de ça trois ans, nous répétions déjà que les technologies évoluaient vite. Force est de constater qu'on n'arrête pas le progrès, et cela appelait bien sûr une troisième édition du *Guide*.

Entre autres scandales, celui des documents confidentiels de la *National Security Agency*², fuités par Edward Snowden³, a permis de prendre la mesure de la panoplie de logiciels malveillants, de matériel espion, et autres systèmes de surveillance, déployés à l'échelle du monde. Les scénarios les plus alarmistes sont finalement le tissu du quotidien en matière de surveillance électronique. Malgré la propagation d'un sentiment d'impuissance, ces différentes révélations sur l'état général de la surveillance numérique rendent d'autant plus nécessaire de se donner les moyens d'y faire face.

L'année 2013 a vu la parution d'études concernant la robustesse toute relative des mots de passe, études qui permettent de mettre fin à d'anciennes intuitions et de bons conseils qui n'en sont plus.

Plusieurs nouveaux avertissements se sont donc glissés ça et là au fil des prochaines pages.

Sur le plan légal, la Loi relative à la Programmation Militaire a été inscrite dans la loi française fin 2013. Cet arsenal élargit les prétextes légaux permettant de surveiller les internautes, le nombre de ministères dont ces requêtes de surveillance peuvent émaner, ainsi que le nombre d'entités auxquelles ces requêtes d'adressent. Elle ouvre également la voie à la collecte *en temps réel* de ces données.

Du côté des outils, le printemps 2013 a vu la sortie de la nouvelle version de Debian, baptisée « *Wheezy* ». En juillet 2014 sortait la version 1.1 du système *live Tails*, dorénavant basé sur Wheezy, et possédant de nouvelles fonctionnalités majeures. Il a donc fallu revoir les outils pour que les recettes fonctionnent sur ces nouveaux systèmes.

La persistance est une de ces nouvelles fonctionnalités. Il est dorénavant possible de conserver, sur une partition chiffrée, des données ainsi que des configurations d'une session à l'autre. L'amnésie n'est plus totale !

La suppression de métadonnées contenues dans de nombreux types de fichiers est désormais simplifiée grâce au logiciel *Metadata Anonymisation Toolkit*, ainsi que la suppression sécurisée de fichiers, tout cela étant maintenant intégré dans Debian.

Enfin le calcul des sommes de contrôles est également simplifié par la mise en place d'un outil graphique permettant de les effectuer.

2. Wikipédia, 2014, *NSA* [<https://fr.wikipedia.org/wiki/NSA>]

3. Wikipédia, 2014, *Edward Snowden* [https://fr.wikipedia.org/wiki/Edward_Snowden]

Et pour les personnes ayant déjà un système installé avec la version précédente de Debian (Squeeze), un nouveau chapitre de cette troisième édition explique comment procéder à la mise à jour vers Debian Wheezy.

Grâce à cette révision, nous espérons que les pages suivantes restent d'une compagnie avisée dans la traversée de la jungle numérique... du moins, jusqu'à la suivante.

Tome 1

Hors connexions

Sommaire

Préface	iii
Les revers de la mémoire numérique	iii
Rien à cacher ?	iii
Comprendre pour pouvoir choisir	iv
Prendre le temps de comprendre	iv
Un « guide »	iv
Préface à la troisième édition	vii
Sommaire	1
I Comprendre	7
<hr/>	
1 Quelques bases sur les ordinateurs	9
1.1 Des machines à traiter les données	9
1.2 Le matériel	9
1.3 Électricité, champs magnétiques et ondes radios	14
1.4 Les logiciels	14
1.5 Le rangement des données	16
2 Traces à tous les étages	19
2.1 Dans la mémoire vive	19
2.2 Dans la mémoire virtuelle	19
2.3 Veille et hibernation	20
2.4 Les journaux	20
2.5 Sauvegardes automatiques et autres listes	21
2.6 Les méta-données	21
3 Malware, mouchards et autres espions	23
3.1 Les logiciels malveillants	24
3.2 Les matériel espions	26
3.3 Les <i>keyloggers</i> , ou enregistreurs de frappe au clavier	26
3.4 Des problèmes d'impression ?	27
4 Quelques illusions de sécurité...	29
4.1 Logiciels propriétaires, <i>open source</i> , libres	29
4.2 Le mot de passe d'un compte ne protège pas ses données	31
4.3 À propos de l'« effacement » des fichiers	32
4.4 Les logiciels portables : une fausse solution	34

5	La cryptographie	37
5.1	Protéger des données des regards indiscrets	37
5.2	S'assurer de l'intégrité de données	41
5.3	Symétrique, asymétrique ?	43
II	Choisir des réponses adaptées	47
<hr/>		
6	Évaluation des risques	49
6.1	Que veut-on protéger ?	49
6.2	Contre qui veut-on se protéger ?	49
7	Définir une politique de sécurité	51
7.1	Une affaire de compromis	51
7.2	Comment faire ?	52
7.3	Quelques règles	52
8	Un nouveau départ	57
8.1	Contexte	57
8.2	Évaluer les risques	57
8.3	Définir une politique de sécurité	58
9	Travailler sur un document sensible	65
9.1	Contexte	65
9.2	Évaluer les risques	65
9.3	Accro à Windows ?	66
9.4	Le système <i>live</i> amnésique	66
9.5	Travailler sur un document sensible... sur un système <i>live</i>	68
9.6	Travailler sur un document sensible... sous Windows	68
9.7	Nettoyer les métadonnées du document terminé	75
9.8	Limites communes à ces politiques de sécurité	75
10	Archiver un projet achevé	77
10.1	Contexte	77
10.2	Est-ce bien nécessaire ?	77
10.3	Évaluer les risques	77
10.4	Méthode	78
10.5	Quelle phrase de passe ?	78
10.6	Un disque dur ? Une clé ? Plusieurs clés ?	79
III	Outils	81
<hr/>		
11	Utiliser un terminal	85
11.1	Qu'est-ce qu'un terminal ?	85
11.2	À propos des commandes	86
11.3	Terminal ? Terminal administrateur ?	88
11.4	Encore une mise en garde	88
11.5	Un exercice	88
11.6	Attention aux traces !	90
11.7	Pour aller plus loin	90
12	Choisir une phrase de passe	91

13 Démarrer sur un CD, un DVD ou une clé USB	93
13.1 Essayer naïvement	93
13.2 Tenter de choisir le périphérique de démarrage	93
13.3 Modifier les paramètres du micrologiciel	94
14 Utiliser un système <i>live</i>	99
14.1 Des systèmes <i>live</i> discrets	99
14.2 Télécharger et installer Tails	100
14.3 Cloner ou mettre à jour une clé Tails	101
14.4 Démarrer sur un système <i>live</i>	101
14.5 Utiliser la persistance de Tails	102
15 Installer un système chiffré	105
15.1 Limites	105
15.2 Télécharger un support d'installation	106
15.3 Vérifier l'empreinte du support d'installation	107
15.4 Préparer les supports d'installation	107
15.5 L'installation proprement dite	110
15.6 Quelques pistes pour continuer	114
15.7 Un peu de documentation sur Debian et GNU/Linux	114
16 Choisir, vérifier et installer un logiciel	115
16.1 Trouver un logiciel	116
16.2 Critères de choix	117
16.3 Installer un paquet Debian	120
16.4 Comment modifier ses dépôts Debian	122
17 Effacer des données « pour de vrai »	127
17.1 Un peu de théorie	127
17.2 Sur d'autres systèmes	128
17.3 Allons-y	128
17.4 Supprimer des fichiers... et leur contenu	129
17.5 Effacer « pour de vrai » tout un disque	129
17.6 Effacer tout le contenu d'un disque	130
17.7 Effacer le contenu d'une partition chiffrée LUKS	132
17.8 Rendre irrécupérables des données déjà supprimées	135
18 Partitionner et chiffrer un disque dur	137
18.1 Chiffrer un disque dur avec LUKS et <code>dm-crypt</code>	137
18.2 D'autres logiciels que l'on déconseille	138
18.3 En pratique	138
18.4 Préparer un disque à chiffrer	139
18.5 Créer une partition non chiffrée	140
18.6 Créer une partition chiffrée	140
18.7 Utiliser un disque dur chiffré	141
19 Sauvegarder des données	143
19.1 Gestionnaire de fichiers et stockage chiffré	143
19.2 En utilisant Déjà Dup	145
20 Partager un secret	149
20.1 Partager une phrase de passe	149
20.2 Reconstituer la phrase de passe	151
21 Utiliser les sommes de contrôle	153
21.1 Obtenir la somme de contrôle d'un fichier	153
21.2 Vérifier l'intégrité d'un fichier	154

22 Installer et utiliser un système virtualisé	155
22.1 Installer VirtualBox	156
22.2 Installer un Windows virtualisé	157
22.3 Sauvegarder une image de disque virtuel propre	160
22.4 Effacer « pour de vrai » une machine virtuelle	161
22.5 Créer une nouvelle machine virtuelle à partir d'une image propre	162
22.6 Envoyer des fichiers à un système virtualisé	164
22.7 Faire sortir des fichiers d'un système virtualisé	166
23 Garder un système à jour	169
23.1 Garder Tails à jour	169
23.2 Garder à jour un système chiffré	169
23.3 Les mises à jour quotidiennes d'un système chiffré	170
23.4 Passage à une nouvelle version stable	170
24 Nettoyer les métadonnées d'un document	175
24.1 Installer les logiciels nécessaires	175
24.2 Ouvrir le <i>Metadata Anonymisation Toolkit</i>	175
24.3 Ajouter des fichiers à nettoyer	175
24.4 Nettoyer les fichiers	176
Qui parle ?	177
Index	179

01 001
100 0010
01
0000111
11100000 0000
00100010 1111
00011 00

000 0010
0000 0011 111
101 01010
1010001 111
000111011 100
10111010 0000
00001 11

0110 0010
10010 1011
011 0011
101010011 1101
101110011
101101 1100
0111 001

000 1111
0111 100 000
000 01010
0101 011
101 11 1011
000 100
00011 000
111001111 10100
110001111 111
00000101 100 1011
001 0100 101 10010
110 0000
001 0001001 0011
1000000 001 001110100 100
101 10 1010 011001
00 010
0000001
100000111 01010
110011000 1000
001110

000 1111
0111 100 000
000 01010
011011100
010001011 0011
0110000 1010
0010

1011 1001
1110 0011
0011 1001
01101100 010
101010001 1111
0010001 0010
1000 10

1100
111 010 1110
0111 1100
01010
01100011 0000
11000010 10101
01110110 00
0011

0011 1000
0010 1100
01111
01001100 010
111010000 10
1111110 0011
1100 00

Comprendre

Devant la grande complexité des outils informatiques et numériques, la quantité d'informations à avaler pour tenter d'acquérir quelques pratiques d'autodéfense peut paraître énorme. Elle l'est sûrement pour qui chercherait à tout comprendre en même temps...

Ce premier tome se concentrera donc sur l'utilisation d'un ordinateur « hors connexion » — on pourrait aussi bien dire *préalablement à toute connexion*. Mais ce sont aussi des connaissances plus générales qui valent *que l'ordinateur soit connecté ou non* à un réseau. On met donc de côté, jusqu'au second tome, les menaces spécifiquement liées à l'usage d'Internet et des réseaux.

Pour ce morceau *hors connexion*, comme pour les autres, on prendra le temps de s'attarder sur des notions de base, leurs implications en termes de sécurité / confidentialité / intimité¹. Après l'analyse de cas concrets d'utilisation, on pourra se pencher sur quelques recettes pratiques.

Une dernière précision avant de nous jeter à l'eau : *l'illusion de sécurité est bien pire que la conscience nette d'une faiblesse*. Aussi, prenons le temps de bien lire les premières parties avant de nous jeter sur nos claviers... ou même de jeter nos ordinateurs par les fenêtres.

1. On souhaite ici faire appel à une notion un peu floue : quelque chose qui tournerait autour de la possibilité de décider ce qu'on révèle, à qui on le révèle, ainsi que ce que l'on garde secret ; quelque chose qui inclurait aussi une certaine attention à déjouer les tentatives de percer ces secrets. Le terme employé en anglais pour nommer ce qu'on évoque ici est *privacy*. Aucun mot français ne nous semble adapté pour porter tout le sens que l'on aimerait mettre derrière cette notion. Ailleurs, on rencontrera souvent le terme « sécurité », mais l'usage qui en est couramment fait nous donne envie de l'éviter.

Quelques bases sur les ordinateurs

Commençons par le commencement.

Un *ordinateur*, ce n'est pas un chapeau de magicien où on peut ranger des lapins et les ressortir quand on a besoin, et qui permettrait en appuyant sur le bon bouton d'avoir une fenêtre ouverte sur l'autre bout du monde.

Un ordinateur est composé d'un ensemble de machines plus ou moins complexes, reliées entre elles par des connexions électriques, des câbles, et parfois des ondes radios. Tout ce *matériel* stocke, transforme et réplique des signaux pour manipuler l'information que l'on peut voir sur un bel écran avec plein de boutons où cliquer.

Comprendre comment s'articulent ces principaux composants, comprendre les bases de ce qui fait fonctionner tout ça, c'est la première étape pour comprendre où sont les forces et les faiblesses de ces engins, à qui l'on confie pas mal de nos données.

1.1 Des machines à traiter les données

Les ordinateurs sont des machines inventées pour pouvoir s'occuper d'informations. Elles savent donc précisément enregistrer, traiter, analyser et classer de l'information, même en très grande quantité.

Dans le monde numérique, copier une information ne coûte que quelques micro-watts, autant dire pas grand'chose : c'est essentiel d'avoir ça en tête si nous voulons limiter l'accès à des informations.

Il faut tout simplement considérer que *mettre une information sur un ordinateur* (et c'est encore plus vrai quand il est sur un réseau), *c'est accepter que cette information puisse nous échapper*.

Ce guide peut aider à limiter la casse, mais il faut malgré tout prendre acte de cette réalité.

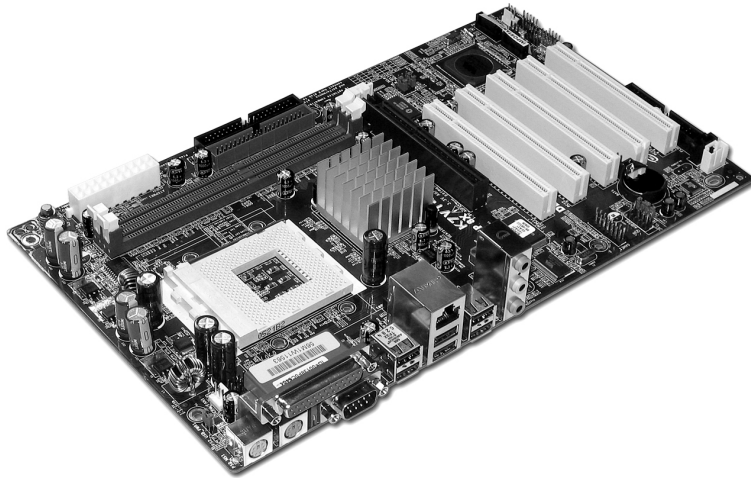
1.2 Le matériel

Somme de composants reliées entre eux, notre ordinateur est donc d'abord une accumulation d'objets, qu'on peut toucher, déplacer, bidouiller, casser.

L'ensemble *écran / clavier / tour* (ou unité centrale), ou l'ordinateur portable, est pratique quand on veut simplement brancher les fils aux bons endroits. Mais pour savoir ce qu'il advient de nos données, un examen plus fin est nécessaire.

On considère ici le contenu d'un ordinateur « classique », parfois appelé PC. Mais on retrouvera la plupart de ces composants avec de légères variations sur d'autres machines : Mac, téléphone portable, « box » de connexion à Internet, tablette, lecteur MP3, *etc.*

1.2.1 La carte-mère



Une carte-mère

Un ordinateur est surtout composé d'éléments électroniques. La *carte-mère* est un gros circuit imprimé qui permet de relier la plupart de ces éléments à travers l'équivalent de fils électriques. Sur la carte-mère viendront se brancher au minimum un processeur, de la mémoire vive, un système de stockage (disque dur ou autre mémoire), de quoi démarrer l'ordinateur (un micrologiciel) et d'autres cartes et périphériques selon les besoins.

On va rapidement faire un petit tour à travers tout ça pour avoir une vague idée de qui fait quoi, ce sera fort utile par la suite.

1.2.2 Le processeur



La puce d'un microprocesseur Intel Pentium 60 Mhz dans son boîtier

Le processeur (aussi appelé CPU, pour *central processing unit* ou « unité centrale de traitement » en français) est le composant qui s'occupe du traitement des données.

Pour se représenter le travail d'un processeur, l'exemple le plus concret sur lequel se baser est la calculatrice. Sur une calculatrice on entre des données (les nombres) et des opérations à faire dessus (addition, multiplication ou autres) avant d'examiner le résultat, éventuellement pour s'en servir ensuite comme base pour d'autres calculs.

Un processeur fonctionne exactement de la même manière. À partir de données (qui peuvent être la liste d'opérations à effectuer), il se contente d'exécuter à la chaîne les traitements à faire. Il ne fait que ça, mais il le fait vraiment très vite.

Mais si le processeur n'est qu'une simple calculatrice, comment peut-on alors effectuer des traitements sur des informations qui ne sont pas des nombres, par exemple sur du texte, des images, du son ou un déplacement de la souris ?

Tout simplement en transformant en nombre tout ce qui ne l'est pas, en utilisant un code défini auparavant. Pour du texte, ça peut par exemple être $A = 65$, $B = 66$, etc. Une fois ce code défini, on peut *numériser* notre information. Avec le code précédent, on peut par exemple transformer « GUIDE » en 71, 85, 73, 44, 69.

Cette série de chiffres permet de représenter les lettres qui composent notre mot. Mais le processus de numérisation perdra toujours de l'information. Pour cet exemple, on perd au passage la spécificité de l'écriture manuscrite alors que pourtant, une rature, des lettres hésitantes constituent tout autant de « l'information ». Lorsque des choses passent dans le tamis du monde numérique, on perd forcément toujours des morceaux au passage.

Au-delà des données, les opérations que le processeur doit effectuer (ses *instructions*) sont également codées sous forme de nombres binaires. Un programme est donc une série d'instructions, manipulées comme n'importe quelles autres données.

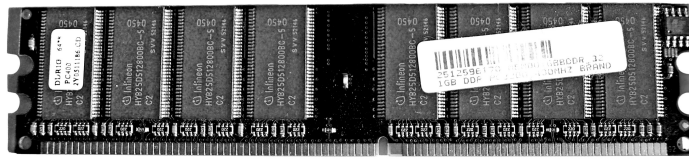
À l'intérieur de l'ordinateur, tous ces nombres sont eux-mêmes représentés à l'aide d'états électriques : absence de courant, ou présence de courant. Il y a donc deux possibilités, ces fameux 0 et 1 que l'on peut croiser un peu partout. C'est pourquoi on parle de *bi*-naire. Et c'est uniquement à l'aide d'un paquet de fils et de plusieurs milliards de *transistors* (des interrupteurs, pas si différents de ceux pour allumer ou éteindre la lumière dans une cuisine) que le traitement des données se fait.

Tous les processeurs ne fonctionnent pas de la même manière. Certains ont été conçus pour être plus efficaces pour certains types de calcul, d'autres pour consommer le moins d'énergie, etc. Par ailleurs, tous les processeurs ne disposent pas exactement des mêmes instructions. Il en existe de grandes familles, que l'on appelle des *architectures*. Cela a son importance, car un programme prévu pour fonctionner sur une architecture donnée ne fonctionnera en général pas sur une autre.

1.2.3 La mémoire vive

La mémoire vive (ou RAM, pour *Random Access Memory*) se présente souvent sous forme de *barrettes*, et se branche directement sur la carte-mère.

La mémoire vive sert à stocker tous les logiciels et les documents ouverts. C'est à cet endroit que le processeur va chercher les données à traiter et entreposer le résultat des opérations. Ces informations doivent donc forcément s'y trouver sous une forme directement utilisable pour effectuer les calculs.



Une barrette de mémoire vive

L'accès à la mémoire vive est très rapide : il suffit du temps nécessaire pour basculer les interrupteurs qui vont relier le processeur à la case de la mémoire à lire (ou à écrire).

Lorsque la mémoire vive n'est plus alimentée en électricité, les données qu'elle contient deviennent illisibles après quelques minutes ou quelques heures, selon les modèles.

1.2.4 Le disque dur



Un disque dur 3 pouces $\frac{1}{2}$

Étant donné que la mémoire vive s'efface à partir du moment où elle n'a plus de courant, l'ordinateur a besoin d'un autre endroit où stocker données et programmes entre chaque allumage. On parle aussi de mémoire *persistante* ou de mémoire *morte* : une mémoire où les informations écrites restent, même sans alimentation électrique.

Pour ce faire, on utilise en général un *disque dur*. C'est souvent une coque en métal dans laquelle se trouvent plusieurs disques qui tournent sans s'arrêter. Sur ces disques se trouvent de minuscules morceaux de fer. Au-dessus de chaque disque se trouvent des *têtes de lecture*. À l'aide de champs magnétiques, ces dernières détectent et modifient la position des morceaux de fer. C'est la position des morceaux de fer qui permet de coder les informations à stocker.

Ce mécanisme est *beaucoup plus lent* — 50 fois environ — que l'accès à la mémoire vive. Par contre, c'est plus simple d'y mettre *beaucoup plus d'informations*.

Les informations que l'on met donc généralement sur un disque dur sont, bien entendu, des documents, mais aussi les programmes et toutes les données qu'ils utilisent pour

fonctionner, comme des fichiers temporaires, des journaux de bord, des fichiers de sauvegarde, des fichiers de configuration, *etc.*

Le disque dur conserve donc une mémoire quasi-permanente et quasi-exhaustive pour toutes sortes de traces qui parlent de nous, de ce que nous faisons, avec qui et comment, dès qu'on utilise un ordinateur.

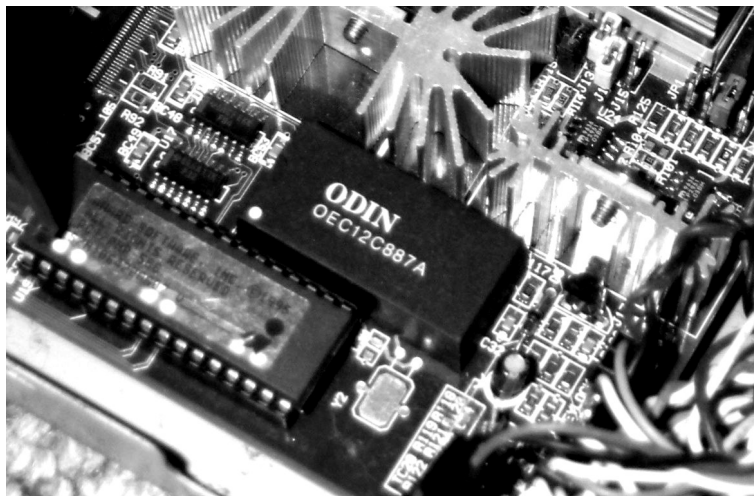
1.2.5 Les autres périphériques

Avec uniquement un processeur, de la mémoire vive et un support de stockage, on obtient déjà un ordinateur. Pas très causant, par contre. Donc on lui adjoint généralement d'autres *périphériques* comme un clavier, une souris, un écran, un adaptateur réseau (avec ou sans fil), un lecteur de DVD, *etc.*

Certains périphériques nécessitent des puces supplémentaires afin que le processeur puisse y accéder. Ces puces peuvent être soudées directement au circuit de la carte-mère (c'est typiquement le cas pour le clavier) ou alors nécessiter l'ajout d'un circuit supplémentaire, livré sous forme de carte (dite *fillette*).

Afin de réduire le nombre de puces spécifiques (et donc coûteuses et compliquées à mettre au point), les systèmes d'accès aux périphériques tendent à s'uniformiser. Par exemple, la norme USB (pour *Universal Serial Bus*) est de plus en plus utilisée pour connecter imprimantes, claviers, souris, disques durs supplémentaires, adaptateurs réseaux ou ce qu'on appelle couramment des « clés USB ».

1.2.6 Le micrologiciel



Une puce de micrologiciel Award BIOS sur une carte-mère

Pour démarrer l'ordinateur, il faut donner au processeur un premier programme, pour pouvoir charger les programmes à exécuter ensuite.

Ce petit logiciel, appelé micrologiciel (*firmware* en anglais) est contenu dans une puce mémoire sur la carte mère. Cette mémoire fait partie d'un troisième type : la mémoire *flash*. C'est une mémoire qui garde les informations lorsqu'elle est éteinte, mais dont on ne peut remplacer le contenu que lors d'une opération qu'on appelle *flashage*. C'est aussi ce type de mémoire qu'on trouve dans les « clés USB » ou les « disques durs » dits *Solid State Disk* (ou SSD).

Le micrologiciel historique de la plupart des ordinateurs personnels était appelé BIOS (*Basic Input/Output System*, ou système d'entrée/sortie de base). Depuis 2012, de plus en plus d'ordinateurs utilisent un nouveau standard appelé UEFI (*Unified Extended Firmware Interface*).

page ci-contre

Ce premier programme qu'exécute l'ordinateur permet, entre autres, de choisir où se trouve le système d'exploitation que l'on veut utiliser (qui sera chargé à partir d'un disque dur, d'une clé USB, d'un CD ou d'un DVD, voire à partir du réseau).

1.3 Électricité, champs magnétiques et ondes radios

En ce qui concerne la confidentialité des informations qui circulent au sein d'un ordinateur, il faut déjà prendre acte de plusieurs choses après ce rapide tour de ce qui le compose.

Tout d'abord, l'essentiel de l'information circule sous forme de courants électriques. Rien n'empêche donc de mettre l'équivalent d'un bête *voltmètre* pour mesurer le courant qui passe, et ainsi pouvoir reconstituer n'importe quelles données manipulées par l'ordinateur sous une forme ou une autre.

Par ailleurs, tout courant qui circule a tendance à émettre un champ magnétique. Ces champs magnétiques peuvent rayonner à quelques mètres, voire plus¹. Il est donc possible pour qui s'en donne les moyens de reconstituer le contenu d'un écran ou ce qui a été tapé sur un clavier, et cela, même derrière un mur, depuis la rue ou l'appartement contigu : ainsi, des chercheurs ont réussi à enregistrer les touches tapées sur des claviers filaires normaux à partir de leurs émissions électromagnétiques, à une distance allant jusqu'à 20 mètres².

Le même type d'opération est possible à partir de l'observation des légères perturbations³ que génère l'ordinateur sur le réseau électrique où il est branché. Il faut toutefois pour cela que l'attaquant soit branché sur le même réseau électrique.

Enfin, certains périphériques (claviers, souris, écouteurs, *etc.*) fonctionnent *sans fil*. Ils communiquent alors avec l'ordinateur par des ondes radio que n'importe qui autour peut capter et éventuellement décoder sans vergogne.

Bref, pour résumer, même si un ordinateur n'est pas connecté à un réseau, et quels que soient les programmes qui fonctionnent, il reste tout de même possible pour des personnes bien équipées de réaliser une « écoute » de ce qui se passe à l'intérieur de l'ordinateur.

1.4 Les logiciels

Au-delà de la somme d'éléments *physiques* qui constituent un ordinateur, il faut aussi se pencher sur les éléments moins palpables : les logiciels.

À l'époque des tout premiers ordinateurs, chaque fois qu'il fallait exécuter des traitements différents, il fallait intervenir physiquement pour changer la disposition des câbles et des composants. On en est bien loin aujourd'hui : les opérations à réaliser pour faire les traitements sont devenues des données comme les autres. Des données qu'on appelle « programmes » qui sont chargées, modifiées, manipulées par d'autres programmes.

Ceux-ci sont généralement écrits pour essayer de ne faire qu'une seule chose, et de la faire bien, principalement dans le but de rester compréhensibles par les êtres humains qui les conçoivent. C'est ensuite l'interaction de dizaines de milliers de programmes

1. Berke Durak a réussi en 1995 à capter les ondes électromagnétiques [<http://lambda-diode.com/electronics/tempest/>] émises par la plupart des composants de son ordinateur avec un simple *walkman* capable de recevoir la radio.

2. Martin Vuagnoux et Sylvain Pasini ont réalisé d'effrayantes vidéos [<http://lasecwww.epfl.ch/keyboard/>] pour illustrer leur papier *Compromising Electromagnetic Emanations of Wired and Wireless Keyboards* publié en 2009.

3. Paul Kocher, Joshua Jaffe et Benjamin Jun ont publié en 1998, en anglais, un rapport [<http://www.cryptography.com/public/pdf/DPATechInfo.pdf>] expliquant les différentes techniques d'analyse de consommation électrique.

entre eux qui permettra de réaliser les tâches complexes pour lesquelles sont généralement utilisés les ordinateurs de nos jours.

L'effet produit lorsqu'on clique sur un bouton, c'est donc le lancement d'une chaîne d'événements, d'une somme impressionnante de calculs, qui aboutissent à des impulsions électriques venant à la fin modifier un objet physique (comme un DVD qu'on veut graver, un écran qui modifie ses LEDs pour afficher une nouvelle page, ou un disque dur qui active ou désactive des micro-interrupteurs pour créer la suite binaire de données qui constituera un *fichier*).

1.4.1 Le système d'exploitation

Le but d'un système d'exploitation est avant tout de permettre aux logiciels de se partager l'accès aux composants matériels de l'ordinateur. Son rôle est aussi de permettre aux différents logiciels de communiquer entre eux. Un système d'exploitation est par ailleurs généralement livré avec des logiciels, au minimum de quoi permettre de démarrer d'autres logiciels.

La partie la plus fondamentale d'un système d'exploitation est son noyau, qui s'occupe de coordonner l'utilisation du matériel par les programmes.

Pour chaque composant matériel de l'ordinateur que l'on veut utiliser, le noyau active un programme qu'on appelle « pilote » (ou *driver* en anglais). Il existe des pilotes pour les périphériques d'entrée (comme le clavier et la souris), de sortie (écran, imprimante, *etc.*), de stockage (DVD, clé USB, *etc.*).

Le noyau gère aussi l'exécution des programmes, en leur donnant des morceaux de mémoire et en répartissant le temps de calcul du processeur entre les différents programmes qui veulent le faire travailler.

Au-delà du noyau, les systèmes d'exploitation utilisés de nos jours, comme Windows, Mac OS X ou GNU/Linux (avec Debian, Ubuntu, Fedora, par exemple) incluent aussi de nombreux utilitaires ainsi que des environnements de bureaux graphiques qui permettent d'utiliser l'ordinateur en cliquant simplement sur des boutons.

Le système d'exploitation est en général stocké sur le disque dur. Cependant, il est aussi tout à fait possible d'utiliser un système d'exploitation enregistré sur une clé USB ou gravé sur un DVD. Dans ce dernier cas, on parle de système *live* (vu qu'aucune modification ne pourra être faite sur le DVD).

1.4.2 Les applications

On appelle « applications » les logiciels qui permettent réellement de faire ce qu'on a envie de demander à l'ordinateur. On peut citer comme exemple Mozilla Firefox comme navigateur web, LibreOffice pour la bureautique ou encore GIMP ou Adobe Photoshop pour le traitement d'images.

Chaque système d'exploitation définit une méthode bien spécifique pour que les applications puissent accéder au matériel, à des données, au réseau, ou à d'autres ressources. Les applications que l'on souhaite utiliser doivent donc être conçues pour le système d'exploitation de l'ordinateur sur lequel on veut s'en servir.

1.4.3 Les bibliothèques

Plutôt que de réécrire dans toutes les applications des morceaux de programme chargés de faire les mêmes choses, les logiciels se les partagent dans des bibliothèques, ou *libraries* en anglais.

Il existe des bibliothèques pour l'affichage graphique (assurant une cohérence de ce qui est affiché à l'écran), pour lire ou écrire des formats de fichiers, pour interroger certains services réseaux, *etc.*

Si l'on n'est pas programmeur, on a rarement besoin de toucher aux bibliothèques. Il peut toutefois être intéressant de connaître leur existence, ne serait-ce que parce qu'un problème (comme une erreur de programmation) dans une bibliothèque peut se répercuter sur tous les logiciels qui l'utilisent.

1.5 Le rangement des données

On a vu qu'un disque dur (ou une clé USB) permettait de garder des données entre deux allumages d'un ordinateur.

Mais, histoire de s'y retrouver, les données sont agencées d'une certaine manière : un meuble dans lequel on aurait simplement entassé des feuilles de papier ne constitue pas vraiment une forme de rangement des plus efficaces...

1.5.1 Les partitions

Tout comme dans un meuble on peut mettre plusieurs étagères, on peut « découper » un disque dur en plusieurs *partitions*.

Chaque étagère pourra avoir une hauteur différente, un classement différent, selon que l'on souhaite y mettre des livres ou des classeurs, par ordre alphabétique ou par ordre de lecture.

De la même manière, sur un disque dur, chaque partition pourra être de taille différente et contenir un mode d'organisation différent : un système de fichiers.

1.5.2 Les systèmes de fichiers

Un système de fichiers sert avant tout à pouvoir retrouver des informations dans notre immense pile de données, comme la table des matières d'un livre de cuisine permet directement d'aller à la bonne page pour lire la recette du festin du soir.

Il peut être important de noter que la suppression d'un fichier ne fait qu'enlever une ligne dans la table des matières. En parcourant toutes les pages, on pourra toujours retrouver notre recette, tant que la page n'aura pas été réécrite — on développera cela plus tard.

[page 32]

On peut imaginer des milliers de formats différents pour ranger des données, et il existe donc de nombreux systèmes de fichiers différents. On parle de *formatage* lors de la création d'un système de fichiers sur un support.

Vu que c'est le système d'exploitation qui donne aux programmes l'accès aux données, un système de fichiers est souvent fortement lié à un système d'exploitation particulier.

Pour en citer quelques-un : les type NTFS, FAT32 sont ceux employés habituellement par les systèmes d'exploitation Windows ; le type *ext* (*ext3*, *ext4*) est souvent utilisé sous GNU/Linux ; les types HFS, HFS+ et HFSX sont employés par Mac OS X.

Il est néanmoins possible de lire un système de fichiers « étranger » au système qu'on utilise, moyennant l'usage du logiciel adéquat. Windows est par exemple capable de lire une partition *ext3*, si on installe le logiciel approprié.

Une des conséquences de cela, c'est qu'il peut exister sur un ordinateur donné des espaces de stockage invisibles pour l'utilisateur parce que non reconnus par le système d'exploitation (ou non accessibles pour l'utilisateur), mais qui sont pourtant bel et bien présents.

1.5.3 Les formats de fichiers

Les données que l'on manipule sont généralement regroupées sous forme de fichiers. Un fichier a un contenu, mais aussi un nom, un emplacement (le dossier dans lequel il se trouve), une taille, et d'autres détails selon le système de fichiers utilisé.

Mais à l'intérieur de chaque fichier, les données sont elles-mêmes organisées différemment selon leur nature et les logiciels utilisés pour les manipuler. On parle de *format* de fichier pour les différencier.

En général, on met à la fin d'un fichier un code, qu'on appelle parfois *extension*, permettant d'indiquer le format du fichier.

Quelques exemples d'extensions : pour la musique, on utilisera le format MP3 ou Ogg, pour un document texte le LibreOffice ce sera OpenDocument Text (ODT), pour des images, on aura le choix entre le JPEG, le PNG, le format d'Adobe Photoshop (PSD), *etc.*

Il peut être intéressant de faire la différence entre les formats *ouverts*, dont les détails sont publics, et les formats *propriétaires*, souvent conçus pour être manipulés par un logiciel bien précis.

Les formats propriétaires ont parfois été observés à la loupe pour être ouverts par d'autres logiciels, mais leur compréhension reste souvent imparfaite et assujettie à des changements d'une version à l'autre d'une application. C'est typiquement le cas pour le format de Microsoft Word, souvent appelé `.doc` ou `.docx`.

1.5.4 La mémoire virtuelle (*swap*)

Normalement, toutes les données auxquelles le processeur doit accéder, et donc tous les programmes et les documents ouverts, devraient se trouver en mémoire vive. Mais pour pouvoir ouvrir plein de programmes et de documents, les systèmes d'exploitation modernes trichent : ils échangent, quand c'est nécessaire, des morceaux de mémoire vive avec un espace du disque dur dédié à cet effet. On parle alors de « mémoire virtuelle », de *swap* en anglais ou encore d'« espace d'échange ».

Le système d'exploitation fait donc sa petite cuisine pour que le processeur ait toujours dans la mémoire vive les données auxquelles il veut réellement accéder. La *swap* est ainsi un exemple d'espace de stockage auquel on ne pense pas forcément, enregistré sur le disque dur, soit sous forme d'un gros fichier contigu (sous Microsoft Windows), soit dans une partition à part (avec Linux).

On reviendra dans la partie suivante sur les problèmes que posent ces questions de format et d'espaces de stockage en termes de confidentialité des données.

Traces à tous les étages

Le fonctionnement normal d'un ordinateur laisse de nombreuses traces de ce que l'on fait dessus. Parfois, elles sont *nécessaires* à son fonctionnement. D'autres fois, ces informations sont collectées pour permettre aux logiciels d'être « plus pratiques ».

2.1 Dans la mémoire vive

On vient de voir que le premier lieu de stockage des informations sur l'ordinateur est la mémoire vive.

page 11

Tant que l'ordinateur est sous tension électrique, elle contient toutes les informations dont le système a besoin. Elle conserve donc nécessairement de nombreuses traces : frappes au clavier (y compris les mots de passe), fichiers ouverts, événements divers qui ont rythmé la phase d'éveil de l'ordinateur.

En prenant le contrôle d'un ordinateur qui est allumé, il n'est pas très difficile de lui faire cracher l'ensemble des informations contenues dans la mémoire vive, par exemple vers une clé USB ou vers un autre ordinateur à travers le réseau. Et prendre le contrôle d'un ordinateur peut être aussi simple qu'y brancher un *iPod* quand on a le dos tourné¹. Une fois récupérées, les nombreuses informations que contient la mémoire vive sur l'ordinateur et les personnes qui l'utilisent pourront alors être exploitées...

Par ailleurs, si ces données deviennent illisibles lors de la mise hors tension, cela prend néanmoins du temps, ce qui peut suffire pour qu'une personne mal intentionnée ait le temps de récupérer ce qui s'y trouve. On appelle cela une « *cold boot attack* » : l'idée est de copier le contenu de la mémoire vive avant qu'elle ait eu le temps de s'effacer, de manière à l'exploiter par la suite. Il est même techniquement possible de porter à très basse température la mémoire d'un ordinateur fraîchement éteint — auquel cas on peut faire subsister son contenu plusieurs heures, voire plusieurs jours².

Cette attaque doit cependant être réalisée peu de temps après la mise hors tension. Par ailleurs, si on utilise quelques gros logiciels (par exemple en retouchant une énorme image avec Adobe Photoshop ou GIMP) avant d'éteindre son ordinateur, les traces qu'on a laissées précédemment en mémoire vive ont de fortes chances d'être recouvertes. Mais surtout, il existe des logiciels spécialement conçus pour écraser le contenu de la mémoire vive avec des données aléatoires.

2.2 Dans la mémoire virtuelle

Comme expliqué auparavant, le système d'exploitation utilise, dans certains cas, une

page 17

1. Maximillian Dornseif, 2004, *Owned by an iPod* [<https://pacsec.jp/psj04/psj04-dornseif-e.ppt>]. Bruce Schneier, 2006, *Hacking Computers Over USB* [http://www.schneier.com/blog/archives/2006/06/hacking_compute.html] (en anglais).

2. J. Alex Halderman et Al., 2008, *Least We Remember : Cold Boot Attacks on Encryption Keys* [<http://citp.princeton.edu/memory/>] (en anglais).

partie du disque dur pour venir en aide à sa mémoire vive. Ça arrive en particulier si l'ordinateur est fortement sollicité, par exemple quand on travaille sur de grosses images, mais aussi dans de nombreux autres cas, de façon peu prévisible.

La conséquence la plus gênante de ce système pourtant bien pratique, c'est que l'ordinateur va écrire sur le disque dur des informations qui se trouvent dans la mémoire vive... informations potentiellement sensibles, donc, *et qui resteront lisibles après avoir éteint l'ordinateur.*

[page 34]

Avec un ordinateur configuré de façon standard, il est donc illusoire de croire qu'un document lu à partir d'une clé USB, même ouvert avec un logiciel portable, ne laissera jamais de traces sur le disque dur.

[page 37]

Pour éviter de laisser n'importe qui accéder à ces données, il est possible d'utiliser un système d'exploitation configuré pour chiffrer la mémoire virtuelle.

2.3 Veille et hibernation

La plupart des systèmes d'exploitation permettent de mettre un ordinateur « en pause ». C'est surtout utilisé avec les ordinateurs portables mais c'est également valable pour les ordinateurs de bureau.

Il y a deux grandes familles de « pause » : la veille et l'hibernation.

2.3.1 La veille

La *veille* (appelée aussi en anglais *suspend to ram* ou *suspend*) consiste à éteindre le maximum de composants de l'ordinateur tout en gardant sous tension de quoi pouvoir le rallumer rapidement.

[page 37]

Au minimum, la mémoire vive continuera d'être alimentée pour conserver l'intégralité des données sur lesquelles on travaillait — c'est-à-dire notamment les mots de passe et les clés de chiffrement.

Bref, un ordinateur en veille protège aussi peu l'accès aux données qu'un ordinateur allumé.

2.3.2 L'hibernation

L'*hibernation* ou *mise en veille prolongée*, appelée aussi en anglais *suspend to disk*, consiste à sauvegarder l'intégralité de la mémoire vive sur le disque dur pour ensuite éteindre complètement l'ordinateur. Lors de son prochain démarrage, le système d'exploitation détectera l'hibernation, re-copiera la sauvegarde vers la mémoire vive et recommencera à travailler à partir de là.

[page 17]

Sur les systèmes GNU/Linux, la copie de la mémoire se fait généralement dans la swap. Sur d'autres systèmes, ça peut être dans un gros fichier, souvent caché.

Vu que c'est le contenu de la mémoire vive qui est écrite sur le disque dur, ça veut dire que tous les programmes et documents ouverts, mots de passe, clés de chiffrement et autres, pourront être retrouvés par quiconque accèdera au disque dur. Et cela, aussi longtemps que rien n'aura été réécrit par-dessus.

[page 37]

Ce risque est toutefois limité par le chiffrement du disque dur : la phrase de passe sera alors nécessaire pour accéder à la sauvegarde de la mémoire vive.

2.4 Les journaux

Les systèmes d'exploitation ont une forte tendance à écrire dans leur journal de bord un historique détaillé de ce qu'ils fabriquent.

Ces journaux (aussi appelés *logs*) sont utiles au système d'exploitation pour fonctionner, et permettent de corriger des problèmes de configuration ou des *bugs*.

Cependant leur existence peut parfois être problématique. Les cas de figure existants sont nombreux, mais les quelques exemples suivants devraient être suffisants pour donner une idée de ce risque :

- sous GNU/Linux, le système garde la date, l'heure et le nom de l'utilisateur qui se connecte chaque fois qu'un ordinateur est allumé ;
- toujours sous GNU/Linux, la marque et le modèle de chaque support amovible (disque externe, clé USB...) branché sont habituellement conservés ;
- sous Mac OS X, la date d'une impression et le nombre de pages sont inscrits dans les journaux ;
- sous Windows, le *moniteur d'évènements* enregistre le nom du logiciel, la date et l'heure de l'installation ou de la désinstallation d'une application.

2.5 Sauvegardes automatiques et autres listes

En plus de ces journaux, il est possible que d'autres traces de fichiers, même supprimés, subsistent sur l'ordinateur. Même si les fichiers et leur contenu ont été bien supprimés, une partie du système d'exploitation ou d'un autre programme peut en garder une trace délibérée.

Voici quelques exemples :

- sous Windows, Microsoft Office peut garder la référence d'un nom de fichier déjà supprimé dans le menu des « documents récents », et parfois même garder des fichiers temporaires avec le contenu du fichier en question ;
- sous GNU/Linux, un fichier d'historique peut contenir le nom d'un fichier préalablement supprimé. Et LibreOffice peut garder autant de traces d'un fichier supprimé que Microsoft Office. En pratique, il existe des dizaines de programmes fonctionnant ainsi ;
- lorsqu'on utilise une imprimante, le système d'exploitation copie souvent le fichier en attente dans la « file d'impression ». Le contenu de ce fichier, une fois la file vidée, n'aura pas disparu du disque dur pour autant ;
- sous Windows, lorsqu'on connecte un lecteur amovible (clé USB, disque dur externe, CD ou DVD), le système commence souvent par explorer son contenu afin de proposer des logiciels adaptés à sa lecture : cette exploration automatique laisse en mémoire la liste de tous les fichiers présents sur le support employé, même si aucun des fichiers qu'il contient n'est consulté.

Il est difficile de trouver une solution adéquate à ce problème. Un fichier, même parfaitement supprimé, continuera probablement à exister sur l'ordinateur pendant un certain temps sous une forme différente. Une recherche sur les données brutes du disque permettrait de voir si des copies de ces données existent ou pas... sauf si elles y sont seulement référencées, ou stockées sous une forme différente ; sous forme compressée, par exemple.

En fait, seul l'écrasement de la totalité du disque et l'installation d'un nouveau système d'exploitation permettent d'avoir la garantie que les traces d'un fichier ont bien été supprimées. Et dans une autre perspective, l'utilisation d'un système *live*, dont l'équipe de développement porte une attention particulière à cette question, garantit que ces traces ne seront pas laissées ailleurs que dans la mémoire vive. Nous y reviendrons.

[page 127]

2.6 Les méta-données

En plus des informations contenues dans un fichier, il existe des informations accompagnant celui-ci, qui ne sont pas forcément visibles de prime abord : date de création,

nom du logiciel, de l'ordinateur, *etc.* Ces « données sur les données » s'appellent communément des « méta-données ».

[page 16] Une partie des méta-données est enregistrée par le système de fichiers : le nom du fichier, la date et l'heure de création et de modification, et souvent bien d'autres choses. Ces traces sont laissées sur l'ordinateur (ce qui peut déjà être un problème en soi), mais celles-ci ne sont la plupart du temps pas inscrites dans le fichier.

[page 17] En revanche, de nombreux formats de fichiers conservent également des méta-données à l'intérieur du fichier. Elles seront donc diffusées lors d'une éventuelle copie sur une clé USB, ou lors de l'envoi d'un email ou d'une publication en ligne. Ces informations pourront être connues de quiconque aura accès au fichier.

Les méta-données enregistrées dépendent des formats et des logiciels utilisés. La plupart des fichiers audio permettent d'y enregistrer le titre du morceau et l'interprète. Les traitements de texte ou les PDFs enregistreront un nom d'auteur, la date et l'heure de création, et parfois même l'historique complet des dernières modifications³, et donc, potentiellement, des informations que l'on pensait avoir supprimé...

La palme revient probablement aux formats d'images comme TIFF ou JPEG : ces fichiers de photos créés par un appareil numérique ou un téléphone portable contiennent des méta-données au format EXIF. Ce dernier peut contenir la marque, le modèle et le numéro de série de l'appareil utilisé, mais aussi la date, l'heure et parfois les coordonnées géographiques de la prise de vue, sans oublier une version miniature de l'image. Ce sont d'ailleurs ces méta-données qui mettront fin à la cavale John McAfee, fondateur et ancien patron de la société de sécurité informatique du même nom⁴. Et toutes ces informations ont tendance à rester après être passées par un logiciel de retouche photo. Le cas de la miniature est particulièrement intéressant : de nombreuses photos disponibles sur Internet contiennent encore l'intégralité d'une photo recadrée... et des visages ayant été « floutés ».⁵

[page 175] Pour la plupart des formats de fichiers *ouverts*, il existe toutefois des logiciels pour examiner et éventuellement supprimer les méta-données.

3. Deblock Fabrice, 2006, *Quand les documents Word trahissent la confidentialité* [<http://www.journaldunet.com/solutions/0603/060327-indiscretions-word.shtml>].

4. Big Browser, 2012, *VICE DE FORME - La bourde qui a mené à l'arrestation de John McAfee* [<http://bigbrowser.blog.lemonde.fr/2012/12/12/vice-de-forme-la-bourde-qui-a-mene-a-larrestation-de-john-mcafee/>].

5. Maximilian Dornseif et Steven J. Murdoch, 2004, *Hidden Data in Internet Published Documents* [<http://events.ccc.de/congress/2004/fahrplan/files/316-hidden-data-slides.pdf>] (en anglais).

Logiciels malveillants, mouchards et autres espions

Au-delà des traces que le fonctionnement de tout système d'exploitation laisse au moins le temps où l'ordinateur fonctionne, on peut aussi trouver dans nos ordinateurs tout un tas de *mouchards*. Soit installés à notre insu (permettant par exemple de détourner les journaux vers d'autres fins), soit présents de manière systématique dans les logiciels qu'on aura installés.

[page 20]

Ces mouchards peuvent participer à diverses techniques de surveillance, de la « lutte » contre le « piratage » de logiciels propriétaires, au fichage ciblé d'un individu, en passant par la collecte de données pour des pourriels (*spam*) ou autres arnaques.

[page 29]

La portée de ces dispositifs augmente fortement dès que l'ordinateur est connecté à Internet. Leur installation est alors grandement facilitée si on ne fait rien de spécial pour se protéger, et la récupération des données collectées se fait à distance.

Toutefois les gens qui récoltent ces informations sont inégalement dangereux : ça dépend des cas, de leurs motivations et de leurs moyens. Les proches abusifs¹, les sites Internet à la recherche de consommateurs à cibler, les multinationales comme Microsoft, les gendarmes de Saint-Tropez, ou la *National Security Agency* américaine... autant de structures souvent en concurrence entre elles et ne formant pas une totalité cohérente.

Pour s'introduire dans nos ordinateurs, ils n'ont pas accès aux mêmes passe-partout, et ne savent pas tous manipuler le pied-de-biche aussi bien : par exemple, l'espionnage industriel est une des raisons importantes de la surveillance plus ou moins légale², et, malgré les apparences³, il ne faut pas croire que Microsoft donne toutes les astuces de Windows à la police française.

1. Catherine Armitage, 2014, *Spyware's role in domestic violence* [<http://www.theage.com.au/technology/technology-news/spywares-role-in-domestic-violence-20140321-358sj.html>] parle de l'utilisation des malwares et autres outils technologiques par des proches abusifs ou violents (en anglais).

2. Pour se faire une idée des problématiques liées à l'espionnage industriel Wikipédia, 2014, *Espionnage industriel* [https://fr.wikipedia.org/wiki/Espionnage_industriel].

3. Microsoft, en partenariat avec Interpol, a fabriqué une boîte à outils appelée COFEE (Computer Online Forensic Evidence Extractor) mise à disposition des polices d'une quinzaine de pays. Korben, 2009, *Cofee - La clé sécurité de Microsoft vient d'apparaître sur la toile* [<http://korben.info/cofee-la-cle-securite-de-microsoft-vient-dapparaître-sur-la-toile.html>].

Cependant, les services de sécurité français disposent maintenant des moyens de mettre en place une surveillance informatique très complète en toute légalité, en s'appuyant sur plusieurs « mouchards » présentés par la suite, à travers la Loi d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure (dite LOPPSI 2). Ce texte inclut en effet des dispositions légales inédites permettant, dans le cadre d'une enquête sur des infractions relevant de criminalité ou de la délinquance organisée, d'installer des mouchards pour enregistrer et transmettre ce qui s'affiche à l'écran ou ce qui est entré au clavier d'un ordinateur, sans nécessairement disposer d'un accès physique à la machine, ou en pénétrant dans le domicile de la personne surveillée pour y installer les outils nécessaires⁴.

3.1 Les logiciels malveillants

Les logiciels malveillants⁵ (que l'on appelle également *malwares*) sont des logiciels qui ont été développés dans le but de nuire : collecte d'informations, hébergement d'informations illégales, relai de pourriel *etc.* Les virus informatiques, les vers, les chevaux de Troie, les *spyware*, les *rootkits* (logiciels permettant de prendre le contrôle d'un ordinateur) et les *keyloggers* sont de cette engeance. Certains programmes peuvent appartenir à plusieurs de ces catégories simultanément.

page 26

Afin de s'installer sur un ordinateur, certains logiciels malveillants exploitent les vulnérabilités du système d'exploitation⁶ ou des applications. Ils s'appuient sur des erreurs de conception ou de programmation pour détourner le déroulement des programmes à leur avantage. Malheureusement, de telles « failles de sécurité » ont été trouvées dans de très nombreux logiciels, et de nouvelles sont trouvées constamment, tant par des gens qui cherchent à les corriger que par d'autres qui cherchent à les exploiter.

Un autre moyen courant est d'inciter la personne utilisant l'ordinateur à lancer le logiciel malveillant en le cachant dans un logiciel en apparence inoffensif. C'est ainsi qu'un simple lien vers une vidéo posté sur un réseau social lié à la révolution syrienne amenait en fait les internautes à télécharger un virus contenant un keylogger⁷. L'attaquant n'est alors pas obligé de trouver des vulnérabilités sérieuses dans des logiciels courants. Il est particulièrement difficile de s'assurer que des ordinateurs partagés par de nombreuses personnes ou des ordinateurs qui se trouvent dans des lieux publics, comme une bibliothèque ou un cybercafé, n'ont pas été corrompus : il suffit en effet qu'une seule personne un peu moins vigilante se soit faite avoir...

4. Pour plus de détails, nous recommandons la lecture de ces deux articles ; Marc Rees, 2009, *LOPPSI : la police sera autorisée à installer des chevaux de Troie* [<http://www.pcinpact.com/actu/news/51027-police-opj-cheval-troie-loppi.htm>] et Marc Rees, 2009, *Les chevaux de Troie de la police seront installables à distance* [<http://www.pcinpact.com/actu/news/51077-loppi-chevaux-troie-police-distance.htm>], et éventuellement du texte de loi Légifrance, 2011, *Section 6 bis : De la captation des données informatiques* [<http://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071154&idSectionTA=LEGISCTA000023712495&dateT0exte=20110428>].

5. Toute cette partie est grandement inspirée du passage consacré à la question dans le *Surveillance Self-Defense Guide* [<https://ssd.eff.org/tech/malware>] de l'*Electronic Frontier Foundation*.

6. D'après l'*Internet Storm Center* [<http://isc.sans.org/survivaltime.html>], une installation de Microsoft Windows sur laquelle les mises à jour de sécurité n'ont pas été faites se fait compromettre en moins de 4 minutes si elle est connectée directement à Internet.

7. Eva Galperin et Al., 2014, *Quantum of Surveillance : Familiar Actors and Possible False Flags in Syrian Malware Campaigns* [https://www.eff.org/files/2013/12/28/quantum_of_surveillance4d.pdf] (en anglais).

En outre, la plupart des logiciels malveillants « sérieux » ne laissent pas de signe immédiatement visible de leur présence, et peuvent même être très difficiles à détecter. Le cas sans doute le plus compliqué est celui de failles jusqu'alors inconnues, appelées « exploits 0 day »⁸, et que les logiciels antivirus seraient bien en mal de reconnaître, car pas encore répertoriées. C'est exactement ce genre d'exploitation de failles « 0 day » que la compagnie VUPEN a vendu à la NSA en 2012⁹.

En 2006, Joanna Rutkowska a présenté lors de la conférence *Black Hat* le *malware* nommé « Blue Pill ». Cette démonstration a montré qu'il était possible d'écrire un *rootkit* utilisant les technologies de virtualisation pour tromper le système d'exploitation et rendre ainsi vraiment très difficile d'identifier la présence du *malware*, une fois celui-ci chargé.

Ces logiciels peuvent voler les mots de passe, lire les documents stockés sur l'ordinateur (même les documents chiffrés, s'ils ont été déchiffrés à un moment), réduire à néant des dispositifs d'anonymat sur Internet, prendre des captures d'écran du bureau et se cacher eux-mêmes des autres programmes. Mais ils peuvent également utiliser le micro, la webcam ou d'autres périphériques de l'ordinateur. Il existe un vrai marché spécialisé où l'on peut acheter de tels programmes, personnalisés pour différents objectifs.

page 37

Ces logiciels peuvent concourir à de nombreuses tâches : obtenir des numéros de cartes bancaires, des mots de passe de compte *PayPal*, à envoyer des pourriels ou à participer à attaquer un serveur en le saturant de demandes. Mais ils servent tout aussi bien à espionner des organisations ou des individus spécifiques¹⁰.

Pour donner un exemple venu des États-Unis, le FBI a écrit un logiciel nommé CIPAV pour *Computer and Internet Protocol Address Verifier*. Ce dernier a permis entre autres d'identifier un adolescent de quinze ans ayant envoyé par email des menaces d'attentat contre un lycée de Washington¹¹.

Plus récemment, la loi HADOPI exige des internautes qu'ils « sécurisent » leur connexion, sous peine d'être responsables des usages illicites qui en seraient faits. Pour cela, l'autorité chargée de l'application de la loi eut la bonne idée de proposer aux internautes d'installer *volontairement* un logiciel espion qui enregistrerait un tas de données concernant l'usage de leur connexion, ainsi que celles permettant d'identifier les machines qui l'ont utilisée¹².

Personne ne sait combien d'ordinateurs sont infectés par des logiciels malveillants, mais certains estiment que c'est le cas pour **40 à 90 %** des installations de Windows.

8. Wikipédia, 2014, *Vulnérabilité jour zéro* [https://fr.wikipedia.org/wiki/Vulnérabilité_zero-day].

9. Grégoire Fleurot, 2013, *Espionnage : Vupen, l'entreprise française qui bosse pour la NSA* [<http://www.slate.fr/france/77866/vupen-nsa-espionnage-exploits>].

10. Ministry of Justice of Georgia et Al., 2012, *CYBER ESPIONNAGE Against Georgian Government* [<http://dea.gov.ge/uploads/CERT%20DOCS/Cyber%20Espionage.pdf>] (en anglais).

11. Kevin Poulsen, 2007, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats* [http://www.wired.com/politics/law/news/2007/07/fbi_spyware] (en anglais).

12. Voir les spécifications du logiciel [http://hadopi.fr/download/sites/default/files/page/pdf/Consultation_sur_les%20specifications_fonctionnelles_des_moyens_de_securisation.pdf]

Il est donc fort probable d'en trouver sur le premier Windows que l'on croisera. Jusqu'à présent, utiliser un système d'exploitation minoritaire (tel GNU/Linux) diminue significativement les risques d'infection car ceux-ci sont moins visés, le développement de *malwares* spécifiques étant économiquement moins rentable.

On peut d'ores et déjà évoquer quelques moyens de limiter les risques :

- n'installer (ou n'utiliser) aucun logiciel de provenance inconnue : ne pas faire confiance au premier site web venu¹³ ;
- prendre au sérieux les avertissements des systèmes d'exploitation récents qui tentent de prévenir les utilisateurs lorsqu'ils utilisent un logiciel peu sûr, ou lorsqu'ils indiquent qu'une mise à jour de sécurité est nécessaire ;
- enfin, limiter les possibilités d'installation de nouveaux logiciels : en limitant l'utilisation du compte « administrateur » et le nombre de personnes y ayant accès.

3.2 Les matériel espions

Les adversaires voulant mettre la main sur les secrets contenus par nos ordinateurs peuvent utiliser des logiciels malveillants comme on vient de le voir, mais peuvent tout aussi bien utiliser du matériel espion. Et celui-ci n'a rien à envier au bon vieux James Bond !

Il existe toute une gamme de matériel plus ou moins facilement disponible permettant intrusions ou exfiltration d'information à quasiment tous les niveaux d'un ordinateur. Suite à la révélation de documents confidentiels de la NSA par Edward Snowden, un véritable catalogue du parfait espion informatique a été publié sur le journal allemand Spiegel¹⁴.

Sans en faire un tour exhaustif, on peut découvrir pêle-mêle dans ce catalogue de faux connecteurs USB, permettant de retransmettre sous forme d'ondes radio ce qui transite par ces mêmes connecteurs, des minuscules puces installées dans les câbles reliant écran ou clavier à l'ordinateur et faisant de même, pour qu'un adversaire puisse capter ce qu'on tape ou voit tout en étant à bonne distance. Enfin, pléthore de matériel espion installé dans l'ordinateur, que ce soit au niveau du disque dur, du BIOS, *etc.*

Le tableau n'est pas très encourageant, un véritable audit de son ordinateur demanderait de démonter celui-ci avec très peu de chance de le remonter de telle manière qu'il puisse fonctionner de nouveau. Cela dit, ce matériel n'est pas à la disposition de tous types d'adversaires. De plus, rien n'indique que l'usage d'un tel matériel est devenu monnaie courante, que ce soit pour des raisons de coût, d'installation, ou autres paramètres.

Nous allons quand même nous attarder un peu sur le cas des *keyloggers* qui peuvent entrer à la fois dans la catégorie du matériel espion et des logiciels malveillants.

3.3 Les *keyloggers*, ou enregistreurs de frappe au clavier

Les enregistreurs de frappe au clavier (*keyloggers*), qui peuvent être « matériels » ou « logiciels », ont pour fonction d'enregistrer furtivement tout ce qui est tapé sur un clavier d'ordinateur, afin de pouvoir transmettre ces données à l'agence ou à la personne qui les a installés¹⁵.

13. Ce conseil vaut tout autant pour les personnes utilisant GNU/Linux. En décembre 2009, le site [gnome-look.org](http://lwn.net/Articles/367874/) a diffusé un *malware* [http://lwn.net/Articles/367874/] présenté comme un économiseur d'écran. Ce dernier était téléchargeable sous forme de paquet Debian au milieu d'autres économiseurs et de fonds d'écran.

14. Spiegel, 2013, *Interactive Graphic : The NSA's Spy Catalog* [http://www.spiegel.de/international/world/a-941262.html] (en anglais).

15. security.resist.ca, 2014, *Keystroke Loggers & Backdoors* [http://security.resist.ca/keylog.shtml] (en anglais).

Leur capacité à enregistrer touche par touche ce qui est tapé sur un clavier, contournant ainsi tout dispositif de chiffrement, permet d'avoir directement accès aux phrases, mots de passe et autres données sensibles entrées lorsqu'il y a un enregistreur de frappe sur un clavier. [page 37]

Les *keyloggers* matériels sont des dispositifs reliés au clavier ou à l'ordinateur. Ils peuvent ressembler à des adaptateurs, à des cartes d'extension à l'intérieur de l'ordinateur (PCI ou *mini-PCI*) et même s'intégrer à l'intérieur du clavier¹⁶. Ils sont donc difficiles à repérer si on ne les recherche pas spécifiquement...

Pour un clavier sans fil, il n'y a même pas besoin de *keylogger* pour récupérer les touches entrées : il suffit de capter les ondes émises par le clavier pour communiquer avec le récepteur, puis de casser le chiffrement utilisé, qui est assez faible dans la plupart des cas¹⁷. À moindre distance, il est aussi toujours possible d'enregistrer et de décoder les ondes électromagnétiques émises par les claviers avec un fil, y compris ceux qui sont intégrés dans un ordinateur portable... [page 14]

Les *keyloggers* logiciels sont beaucoup plus répandus, parce qu'ils peuvent être installés à distance (via un réseau, par le biais d'un logiciel malveillant, ou autre), et ne nécessitent généralement pas un accès physique à la machine pour la récupération des données collectées (l'envoi peut par exemple se faire périodiquement par email). La plupart de ces logiciels enregistrent également le nom de l'application en cours, la date et l'heure à laquelle elle a été exécutée ainsi que les frappes de touches associées à cette application.

Aux États-Unis, le FBI utilise depuis de nombreuses années des *keyloggers* logiciels¹⁸.

La seule manière de repérer les *keyloggers* matériels est de se familiariser avec ces dispositifs et de faire régulièrement une vérification visuelle de sa machine, à l'intérieur et à l'extérieur. Même si le catalogue de la NSA publié fin 2013 rend compte de la difficulté de trouver soi-même des dispositifs d'enregistrement de frappe à peine plus gros qu'un ongle. Pour les *keyloggers* logiciels, les pistes sont les mêmes que pour les autres logiciels malveillants. [page 24]

3.4 Des problèmes d'impression ?

On croyait avoir fait le tour des surprises que nous réservent nos ordinateurs... mais même les imprimantes se mettent à avoir leurs petits secrets.

3.4.1 Un peu de stéganographie

Première chose à savoir : de nombreuses imprimantes haut de gamme signent leur travail. Cette signature stéganographique¹⁹ repose sur de très légers détails d'impression, souvent invisibles à l'œil nu, et insérés dans chaque document. Ils permettent d'identifier de manière certaine la marque, le modèle et dans certains cas le numéro de série de la machine qui a servi à imprimer un document. On dit bien « de manière certaine », car c'est pour cela que ces détails sont là : afin de pouvoir retrouver la machine à partir de ses travaux. Toutes les imprimantes ne sont pas pourvues de ce système, baptisé *watermarking*, mais c'est le cas pour nombre de modèles courants²⁰.

16. Pour se faire une idée, nombre de modèles sont en vente libre [<http://www.google.com/products?q=keyloggers>] pour une somme allant de 40 à 100 \$.

17. ZDNet Australia, 2007, *Microsoft wireless keyboard hacked from 50 metres* [<http://www.zdnet.com.au/news/security/soa/Microsoft-wireless-keyboard-hacked-from-50-metres/0,130061744,339284328,00.htm>] (en anglais).

18. En 2000, l'usage d'un *keylogger* a permis au FBI [http://www.theregister.co.uk/2000/12/06/mafia_trial_to_test_fbi/] d'obtenir la phrase de passe utilisée par un pont de la mafia de Philadelphie pour chiffrer ses documents (en anglais).

19. Pour en savoir plus sur la stéganographie, nous conseillons la lecture de cet article Wikipédia, 2014, *Stéganographie* [<https://fr.wikipedia.org/wiki/St%C3%A9ganographie>].

20. L'*Electronic Frontier Foundation* tente de maintenir une liste des constructeurs et de ces modèles d'imprimantes indiscrets [<http://www.eff.org/issues/printers>] (en anglais).

Par ailleurs, d'autres types de traces liées à l'usure de la machine sont aussi laissées sur les documents — et ce avec toutes les imprimantes. Car avec l'âge, les têtes d'impression se décalent, de légères erreurs apparaissent, les pièces s'usent, et tout cela constitue au fur et à mesure une signature propre à l'imprimante. Tout comme la balistique permet d'identifier une arme à feu à partir d'une balle, il est possible d'utiliser ces défauts pour identifier une imprimante à partir d'une page qui en est sortie.

Pour se protéger en partie de cela, il est intéressant de savoir que les détails d'impression ne résistent pas à la photocopie répétée : photocopier la page imprimée, puis photocopier la photocopie obtenue, suffit à faire disparaître de telles signatures. Par contre... on en laissera sûrement d'autres, les photocopieuses présentant des défauts, et parfois des signatures stéganographiques, similaires à ceux des imprimantes. Bref on tourne en rond, et le problème devient surtout de choisir *quelles* traces on veut laisser...

3.4.2 La mémoire, encore...

Certaines imprimantes sont suffisamment « évoluées » pour être plus proches d'un véritable ordinateur que d'un tampon encreur.

[page 11] Elles peuvent poser des problèmes à un autre niveau, vu qu'elles sont dotées d'une mémoire vive : celle-ci, tout comme celle du PC, gardera la trace des documents qui ont été traités aussi longtemps que la machine est sous tension... ou jusqu'à ce qu'un autre document les recouvre.

La plupart des imprimantes lasers disposent d'une mémoire vive pouvant contenir une dizaine de pages. Les modèles plus récents ou ceux comportant des scanners intégrés peuvent, quant à eux, contenir plusieurs milliers de pages de texte...

[page 12] Pire encore : certains modèles, souvent utilisés pour les gros tirages comme dans les centres de photocopies, disposent parfois de disques durs internes, auxquels l'utilisateur n'a pas accès, et qui gardent eux aussi des traces — et cette fois, même après la mise hors tension.

Quelques illusions de sécurité...

Bien. On commence à avoir fait le tour des traces que nous pouvons laisser involontairement, et des informations que des personnes mal intentionnées pourraient nous arracher.

Reste maintenant à pourfendre quelques idées reçues.

4.1 Logiciels propriétaires, *open source*, libres

On a vu qu'un logiciel pouvait faire plein de choses qu'on n'aurait pas du tout envie qu'il fasse. Dès lors, il est indispensable de faire ce que l'on peut pour réduire ce problème autant que possible. De ce point de vue, les logiciels libres sont dignes d'une confiance bien plus grande que les logiciels dits « propriétaires » : nous allons voir pourquoi.

4.1.1 La métaphore du gâteau

Pour comprendre la différence entre logiciels libres et propriétaires, on utilise souvent la métaphore du gâteau. Pour faire un gâteau, il faut une recette : il s'agit d'une liste d'instructions à suivre, des ingrédients à utiliser et d'un procédé de transformation à effectuer. De la même façon, la recette d'un logiciel est appelée « code source ». Elle est écrite dans un langage fait pour être compréhensible par des êtres humains. Cette recette est ensuite transformée en un code compréhensible par le processeur, un peu comme la cuisson d'un gâteau nous donne ensuite la possibilité de le manger.

Les logiciels propriétaires ne sont disponibles que « prêts à consommer », comme un gâteau industriel, sans sa recette. Il est donc très difficile de s'assurer de ses ingrédients : c'est faisable, mais le processus est long et compliqué. Au demeurant, relire une série de plusieurs millions d'additions, de soustractions, de lectures et d'écritures en mémoire pour en reconstituer le but et le fonctionnement est loin d'être la première chose que l'on souhaite faire sur un ordinateur.

Les logiciels libres, au contraire, livrent la recette pour quiconque veut comprendre ou modifier le fonctionnement du programme. Il est donc plus facile de savoir ce qu'on donne à manger à notre processeur, et donc ce qui va s'occuper de nos données.

4.1.2 Les logiciels propriétaires : une confiance aveugle

Un logiciel « propriétaire » est donc un peu comme une « boîte » étanche : on peut constater que le logiciel fait ce qu'on lui demande, possède une belle interface graphique, *etc.* Sauf qu'on ne peut pas vraiment connaître en détail comment il procède ! On ne sait pas s'il se cantonne à faire ce qu'on lui demande, ou s'il fait d'autres choses

en plus. Pour le savoir, il faudrait pouvoir étudier son fonctionnement, ce qui est difficile à faire sans son code source... il ne nous reste donc qu'à lui faire *aveuglément* confiance.

Windows et Mac OS X, les premiers, sont d'immenses boîtes hermétiquement fermées sur lesquelles sont installées d'autres boîtes tout aussi hermétiques (de Microsoft Office aux anti-virus...) qui font peut-être bien d'autres choses que celles qu'on leur demande.

Notamment, balancer des informations que ces logiciels pourraient grappiller sur nous ou permettre d'accéder à l'intérieur de notre ordinateur au moyen de *backdoors*, des « portes dérobées »¹ prévues dans le logiciel pour que ceux qui en ont la clé puissent pirater nos ordinateurs... en fait, vu que l'on ne peut pas savoir comment est écrit le système d'exploitation, on peut tout imaginer en la matière.

Dès lors, laisser reposer la confidentialité et l'intégrité de ses données sur des programmes auxquels on ne peut accorder sa confiance que les yeux fermés, relève de la plus pure illusion de sécurité. Et installer d'autres logiciels prétendant sur leur emballage veiller à cette sécurité à notre place, alors que leur fonctionnement n'est pas plus transparent, ne peut pas résoudre ce problème.

4.1.3 L'avantage d'avoir la recette : les logiciels libres

La confiance plus grande qu'on peut mettre dans un système *libre* comme GNU/Linux est principalement liée au fait de disposer de la « recette » qui permet de le fabriquer. Gardons en tête quand même qu'il n'y a rien de magique : les logiciels libres ne jettent aucun « sort de protection » sur nos ordinateurs.

Toutefois, GNU/Linux offre davantage de possibilités pour rendre un peu plus sûr l'usage des ordinateurs, notamment en permettant de configurer assez finement le système. Ça implique trop souvent des savoirs-faire relativement spécialisés, mais au moins c'est possible.

Par ailleurs, le mode de production des logiciels libres est peu compatible avec l'introduction de portes dérobées : c'est un mode de production collectif, plutôt ouvert et transparent, auquel participent des gens assez variés ; il n'est donc pas facile d'y mettre en toute discrétion des cadeaux à l'attention de personnes mal intentionnées.

Il faut toutefois se méfier des logiciels qualifiés d'*open source*. Ces derniers donnent eux aussi accès à leurs entrailles, mais ont des modes de développement plus fermés, plus opaques. La modification et la redistribution de ces logiciels est au pire interdite, et au mieux autorisée formellement mais rendue en pratique très pénible. Vu que seule l'équipe à l'origine du logiciel va pouvoir participer au développement, on peut considérer que, en pratique, personne ne lira en détail leur code source... et donc que personne ne vérifiera vraiment leur fonctionnement.

C'est le cas par exemple de TrueCrypt, dont le développement s'est arrêté en mai 2014. Logiciel de chiffrement dont le code source est disponible, mais dont le développement est fermé et dont la licence restreint la modification et la redistribution. Pour ce qui nous occupe, le fait qu'un logiciel soit *open source* doit plutôt être considéré comme un argument commercial que comme un gage de confiance.

Sauf que... la distinction entre logiciels libres et *open source* est de plus en plus floue : des employés d'IBM et compagnie écrivent de grosses parties des logiciels libres les plus importants, et on ne va pas toujours regarder de près ce qu'ils écrivent. Par exemple, voici les statistiques des employeurs des gens qui développent le noyau Linux (qui est libre), exprimées en nombre de lignes de code source modifiées, sur une courte période de temps² :

1. Au sujet des « portes dérobées » voir l'article [Wikipédia, 2014, Porte dérobée](https://fr.wikipedia.org/wiki/Porte_dérobée) [https://fr.wikipedia.org/wiki/Porte_dérobée].

2. [Linux Weekly News, 2014, Some 3.14 development statistics](https://lwn.net/Articles/590354/) [https://lwn.net/Articles/590354/] (en anglais).

Organisation	Pourcentage
Linux Foundation	11.4%
Intel	10.0%
(None)	6.8%
Red Hat	6.7%
Texas Instruments	4.1%
(Unknown)	3.7%
IBM	3.7%
Realsil Microelectronics	3.4%
SUSE	3.3%
NVIDIA	3.0%
<i>etc.</i>	

Alors... il n'est pas impossible qu'une personne qui écrit un bout de logiciel dans un coin, et à qui la « communauté du libre » fait confiance, ait pu y glisser des bouts de code mal intentionné. Comme ce fut le cas avec la faille connue sous le nom d'*Heartbleed*³. Si on utilise uniquement des logiciels libres livrés par une distribution GNU/Linux non commerciale, il y a peu de chances que ce cas se présente, mais c'est une possibilité. On fait alors confiance aux personnes travaillant sur la distribution pour étudier le fonctionnement des programmes qui y sont intégrés.

Il est néanmoins important de rappeler que cette confiance ne peut valoir que si on n'installe pas n'importe quoi sur son système. Par exemple, sur Debian, les paquets officiels de la distribution sont « signés », ce qui permet de vérifier leur provenance. Mais si on installe des paquets ou des extensions pour Firefox trouvés sur Internet sans les vérifier, on s'expose à tous les risques mentionnés au sujet des logiciels malveillants.

[page 24]

Pour conclure, et ne pas nous faire plus d'illusions : *libre ou pas, il n'existe pas de logiciel pouvant, à lui seul, assurer l'intimité de nos données*; pour le faire, il n'existe que des pratiques, associées à l'utilisation de *certaines logiciels*. Logiciels choisis parce que des éléments nous permettent de leur accorder un certain niveau de confiance.

4.2 Le mot de passe d'un compte ne protège pas ses données

Tous les systèmes d'exploitation récents (Windows, Mac OS X, GNU/Linux) offrent la possibilité d'avoir différents utilisateurs sur un même ordinateur. Il faut bien savoir que les mots de passe qui protègent parfois ces utilisateurs ne garantissent pas du tout la confidentialité des données.

Certes il peut être pratique d'avoir son espace à soi, avec ses propres réglages (marque-pages, fond d'écran...), mais une personne qui souhaiterait avoir accès à toutes les données qu'il y a sur l'ordinateur n'aurait aucun mal à y parvenir : il suffit de rebrancher le disque dur sur un autre ordinateur ou de le démarrer sur un autre système d'exploitation pour avoir accès à toutes les données écrites sur le disque dur.

[page 15]

Aussi, si utiliser des comptes séparés et des mots de passe peut avoir quelques avantages (comme la possibilité de verrouiller l'écran quand on s'éloigne quelques minutes), il est nécessaire de garder en tête que cela ne protège pas réellement les données.

3. Wikipédia, 2014, *Heartbleed* [<https://fr.wikipedia.org/wiki/Heartbleed>].

4.3 À propos de l'« effacement » des fichiers

page 16

On a déjà évoqué que le contenu d'un fichier devenu inaccessible ou invisible ne s'était pas pour autant volatilisé. On va maintenant détailler pourquoi.

4.3.1 La suppression d'un fichier n'en supprime pas le contenu...

... et ça peut être très facile de le retrouver.

En effet, lorsqu'on « supprime » un fichier — en le plaçant dans la *Corbeille* puis en la vidant — on ne fait que dire au système d'exploitation que le contenu de ce fichier ne nous intéresse plus. Il supprime alors son entrée dans l'index des fichiers existants. Il a ensuite le loisir de réutiliser l'espace que prenaient ces données pour y inscrire autre chose.

Mais il faudra peut-être des semaines, des mois ou des années avant que cet espace soit *effectivement* utilisé pour de nouveaux fichiers, et que les anciennes données disparaissent réellement. En attendant, si on regarde directement ce qui est inscrit sur le disque dur, on retrouve le contenu des fichiers. C'est une manipulation assez simple, automatisée par de nombreux logiciels (qui permettent de « récupérer » ou de « restaurer » des données).

4.3.2 Un début de solution : réécrire plusieurs fois par-dessus les données

Une fois que l'espace d'un disque dur a été réécrit, il devient difficile de retrouver ce qui s'y trouvait auparavant. Mais cela n'est pas pour autant impossible : lorsque l'ordinateur réécrit 1 par-dessus 0, cela donne plutôt 0,95 et lorsqu'il réécrit 1 par-dessus 1, cela donne plutôt 1,05⁴... un peu comme on peut lire sur un bloc-notes ce qui a été écrit sur une page arrachée, par les dépressions créées sur la page vierge située en-dessous.

En revanche ça devient très difficile, voire impossible, de les récupérer quand on réécrit un grand nombre de fois par-dessus, et de différentes manières. La meilleure façon, donc, de rendre inaccessible le contenu de ces fichiers « supprimés », est d'utiliser des logiciels qui s'assureront de le réécrire plusieurs fois, pour terminer par du charabia incompréhensible. C'est ce qu'on appelle « écraser des données » (*wipe* en anglais).

4.3.3 Quelques limites des possibilités de réécriture

Même s'il est possible de réécrire plusieurs fois à un endroit donné d'un disque dur pour rendre inaccessibles les données qu'il contenait, cela ne garantit pas pour autant leur disparition complète du disque...

Les disques « intelligents »

Les disques durs modernes réorganisent leur contenu « intelligemment » : une partie du disque est réservée pour remplacer des endroits qui deviendraient défectueux. Ces opérations de remplacement sont difficilement détectables, et on ne peut jamais être vraiment sûr que l'endroit sur lequel on réécrit trente fois est bien celui où le fichier a été écrit initialement...

Pour les clés USB, on est même sûr que dans la plupart des cas on réécrit à un endroit différent. Comme la mémoire *flash*, utilisée par les clés USB et les disques durs SSD

4. Peter Gutmann, 1996, *Secure Deletion of Data from Magnetic and Solid-State Memory* [http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html] (en anglais).

(*Solid State Disks*), arrête de fonctionner correctement après un certain nombre d'écritures⁵, ces derniers contiennent des puces chargées de réorganiser automatiquement le contenu pour répartir les informations au maximum d'endroits différents.

En prenant en compte ces mécanismes, il devient difficile de garantir que les données que l'on souhaite détruire auront bien disparu.

Néanmoins, ouvrir un disque dur pour en examiner les entrailles demande du temps et d'importantes ressources matérielles et humaines... investissement qui ne sera pas forcément à la portée de tout le monde, tout le temps.

Pour les puces de mémoire *flash* d'une clé USB ou d'un disque dur SSD, même si ce n'est pas non plus immédiat, l'opération est beaucoup plus simple : il suffit d'un fer à souder, et d'un appareil permettant de lire directement les puces de mémoire. Ces derniers se trouvent pour environ 1 500 dollars⁶.

Les systèmes de fichiers « intelligents »

Un autre problème vient des systèmes de fichiers « intelligents ».

[page 16]

Les systèmes de fichiers développés ces dernières années, comme NTFS ou *ext3*, sont « journalisés », c'est-à-dire qu'ils gardent une trace des modifications successives faites sur les fichiers dans un « journal ». Après une extinction brutale de l'ordinateur, cela permet au système de se contenter de reprendre les dernières opérations à faire, plutôt que de devoir parcourir l'intégralité du disque pour corriger les incohérences. Par contre, cela peut ajouter, encore une fois, des traces sur les fichiers que l'on souhaiterait voir disparaître.

[page 20]

Le système de fichiers utilisé actuellement le plus souvent sous GNU/Linux, *ext3*, peut fonctionner avec plusieurs modes. Celui le plus couramment utilisé ne met dans le journal que les noms des fichiers et d'autres méta-données, pas leur contenu.

D'autres techniques, moins courantes sur un ordinateur personnel, peuvent aussi poser problème : les systèmes de fichiers avec écriture redondante et continuant à écrire même en cas d'erreur, comme les systèmes de fichiers RAID ; les systèmes de fichiers qui effectuent des instantanés (*snapshots*) ; les systèmes de fichiers qui mettent en cache dans des dossiers temporaires, comme les clients NFS (système de fichiers par le réseau) ; les systèmes de fichiers compressés⁷.

Enfin, il ne faut pas oublier que le fichier, même parfaitement supprimé, peut avoir laissé des traces ailleurs...

[page 19]

Ce qu'on ne sait pas...

Pour ce qui est des CD-RW ou DVD±RW (ré-inscriptibles), il semble qu'aucune étude sérieuse n'ait été menée à propos de l'efficacité de la réécriture pour rendre des données irrécupérables. Un postulat prudent est donc de détruire méthodiquement les supports de ce type qui auraient pu contenir des données à faire disparaître.

5. Les modèles bas de gamme ne fonctionneront plus correctement après avoir été écrits cent mille fois, et cinq millions pour les meilleurs. D'après Wikipédia, 2014, *Solid-state drive* [https://fr.wikipedia.org/wiki/Solid_State_Drive].

6. Le *Salvation Data Flash Doctor* [<http://www.sd-flash.com/>] ou encore le *PC-3000 Flash SSD Edition* [<http://www.pc-3000flash.com/>] sont tous les deux vendus comme des *outils professionnels de recouvrement de données sur des périphériques flash endommagés* (liens en anglais).

7. *Page de manuel de shred(1)* [<http://manpages.debian.net/cgi-bin/man.cgi?query=shred&locale=fr>].

4.3.4 Plein d'autres fois où l'on « efface »

Il faut noter qu'on ne supprime pas seulement des fichiers en les mettant à la corbeille. Par exemple, quand on utilise l'option « Effacer mes traces » du navigateur Firefox, ce dernier ne fait pas mieux que de *supprimer* les fichiers. Certes les données sont devenues inaccessibles pour Firefox, mais elles sont toujours accessibles en regardant directement le disque dur.

Enfin, il est utile d'insister ici sur le fait que le *reformatage* d'un disque dur n'efface pas pour autant le contenu qui s'y trouvait. De même que la suppression des fichiers, cela ne fait que rendre disponible l'espace où se trouvait le contenu précédemment, les données restant physiquement présentes sur le disque. Tout comme détruire le catalogue d'une bibliothèque ne fait pas pour autant disparaître les livres présents dans les rayonnages...

On peut donc toujours retrouver des fichiers après un reformatage, aussi facilement que s'ils avaient été simplement « supprimés »...

4.3.5 Et pour ne laisser aucune trace ?

Pour régler radicalement le problème, il n'y a pas de méthode simple. La solution la moins difficile pour l'instant est d'utiliser l'ordinateur après l'avoir démarré avec un système *live* configuré pour n'utiliser que la mémoire vive, comme *Tails*. Alors, il est possible de ne rien écrire sur le disque dur ni sur le *swap*, et de ne garder les informations (tant que l'ordinateur est allumé) que dans la mémoire vive.

4.4 Les logiciels portables : une fausse solution

Ce qu'on appelle « logiciels portables », ce sont des logiciels qui ne sont pas installés sur un système d'exploitation donné, mais que l'on peut démarrer depuis une clé USB ou un disque dur externe — et donc, transporter avec soi afin d'en disposer sur n'importe quel ordinateur.

Il est devenu très facile de télécharger sur Internet de telles applications. Des « packs portables » ont ainsi été mis en ligne, comme Firefox avec Tor, ou Thunderbird avec Enigmail.

Toutefois, contrairement aux systèmes *live*, ils se servent du système d'exploitation installé sur l'ordinateur où on les utilise (la plupart du temps, ils sont prévus pour Windows).

L'idée qui est à leur origine est de permettre d'avoir toujours les logiciels dont on a besoin, sous la main, personnalisés à notre usage. Mais « transporter son bureau partout avec soi », par exemple, n'est pas forcément la meilleure manière de préserver la confidentialité de ses données.

Disons-le tout de suite : ces logiciels ne protègent pas plus les personnes qui s'en servent que des logiciels « non portables ». Pire, le discours faisant leur promotion participe à créer une illusion de sécurité avec d'énormes bêtises comme « *l'utilisation des logiciels se fait de façon sécurisée et sans laisser d'informations personnelles sur les machines sur lesquelles vous utilisez votre Framakey.* »⁸. C'est malheureusement faux.

8. Cet extrait provient de la [page d'accueil du site web de Framakey](http://www.framakey.org/) [http://www.framakey.org/], une compilation de logiciels portables réalisée par Framasoft [http://www.framasoft.net/], un site français de promotion du logiciel libre. Sur la [présentation de la Framakey](http://framakey.org/Main/Details) [http://framakey.org/Main/Details], on peut lire maintenant « *le navigateur web et le client mail protégeront votre intimité et l'ordinateur hôte en laissant un minimum de traces* »... sans plus de précisions sur la nature de ces traces.

4.4.1 Principaux problèmes

Ces solutions « clé en main » posent donc quelques problèmes plutôt fâcheux...

Il restera des traces sur le disque dur

Si le logiciel a été rendu « portable » correctement, il ne devrait pas laisser délibérément de traces sur le disque dur de l'ordinateur sur lequel on l'utilise. Mais en fait, le logiciel n'a jamais un contrôle absolu. Il dépend en effet largement du système d'exploitation sur lequel il est employé, qui peut avoir besoin d'écrire de la « mémoire virtuelle » sur le disque dur, ou d'enregistrer diverses traces de ce qu'il fait dans ses journaux et autres « documents récents ». Tout cela restera ensuite sur le disque dur.

[page 19]

[page 20]

[page 21]

Il n'y a aucune raison d'avoir confiance en un système inconnu

On a vu auparavant que beaucoup de systèmes ne faisaient absolument pas ce que l'on croit. Or, puisque le logiciel portable va utiliser le système installé sur l'ordinateur sur lequel on le lance, on souffrira de tous les mouchards et autres logiciels malveillants qui pourraient s'y trouver...

[page 23]

On ne sait pas qui les a compilés, ni comment

Les modifications apportées aux logiciels pour les rendre portables sont rarement vérifiées, alors même qu'elles ne sont généralement pas faites par les auteurs du logiciel lui-même. Dès lors, on peut soupçonner ces logiciels, encore plus que leurs versions non-portables, de contenir des failles de sécurité, qu'elles aient été introduites par erreur ou volontairement.

On traitera plus loin de la question de l'hygiène minimale à avoir dans le choix des logiciels qu'on installe ou télécharge.

Une piste pour se protéger : la cryptographie

La *cryptographie* est la branche des mathématiques qui s'occupe spécifiquement de protéger des messages. Jusqu'en 1999, l'usage de techniques cryptographiques était interdit au grand public. C'est devenu légal entre autres pour permettre aux services marchands sur Internet de se faire payer sans que les clients se fassent piquer leur numéro de carte bleue.

La *cryptanalyse* est le domaine consistant à « casser » les techniques cryptographiques, par exemple pour permettre de retrouver un message qui avait été protégé¹.

Lorsque l'on veut protéger des messages, on distingue trois aspects :

- confidentialité : empêcher les regards indiscrets ;
- authenticité : s'assurer de la source du message ;
- intégrité : s'assurer que le message n'a pas subi de modification.

On peut désirer ces trois choses en même temps, mais on peut aussi vouloir seulement l'une ou l'autre. L'émetteur d'un message *confidentiel* peut souhaiter nier en être l'auteur (et donc qu'on ne puisse pas l'*authentifier*). On peut aussi imaginer vouloir certifier la provenance (*authentifier*) et l'*intégrité* d'un communiqué officiel qui sera diffusé publiquement (donc loin d'être *confidentiel*).

Dans tout ce qui suit, on va parler de *messages*, mais les techniques cryptographiques s'appliquent de fait à n'importe quels nombres, donc à n'importe quelles données, une fois numérisées.

À noter, la cryptographie ne cherche pas à cacher les messages, mais à les protéger. Pour cacher des messages, il est nécessaire d'avoir recours à des techniques stéganographiques (comme celles utilisées par les imprimantes évoquées auparavant), dont nous ne parlerons pas ici.

page 27

5.1 Protéger des données des regards indiscrets

Comme l'ont bien compris les gamins utilisant des codes pour s'échanger des messages ou les militaires communiquant leurs ordres, la piste la plus sérieuse pour que des données ne puissent être comprises que par les personnes « dans le secret », c'est celle du *chiffrement*.

Le chiffrement d'un fichier ou d'un support de stockage permet de le rendre illisible pour toute personne qui n'a pas le code d'accès (souvent une *phrase de passe*). Il sera

1. Pour un bon aperçu des différentes méthodes, qu'on appelle des « attaques », couramment utilisées en cryptanalyse, on peut se référer à la page [Wikipédia, 2014, Cryptanalyse \[https://fr.wikipedia.org/wiki/Cryptanalyse\]](https://fr.wikipedia.org/wiki/Cryptanalyse).

certes toujours possible d'accéder au contenu, mais les données ressembleront à une série de nombres aléatoires, et seront donc illisibles.

Souvent on dit *crypter* et *décrypter* à la place de *chiffrer* et *déchiffrer*, ce qui peut porter à confusion ; les termes sont cependant synonymes.

5.1.1 Comment ça marche ?

Grosso modo, il y a seulement trois grandes idées pour comprendre comment on peut chiffrer des messages².

La première idée : la *confusion*. Il faut obscurcir la relation entre le message original et le message chiffré. Un exemple très simple est le « chiffre de César » :

texte en clair :	ASSAUT	DANS	UNE	HEURE
	↓↓↓↓↓	↓↓↓↓	↓↓↓	↓↓↓↓↓
texte chiffré :	DVVDXW	GDQV	XQH	KHXUH

$$\boxed{A + 3 \text{ lettres} = D}$$

Sauf qu'avec le chiffre de César, il est facile d'analyser la fréquence des lettres et de retrouver les mots.

Alors la deuxième grande idée, c'est la *diffusion*. Cela permet d'éclater le message pour le rendre plus difficile à reconnaître. Un exemple de cette technique, c'est la transposition par colonne :

$$\begin{pmatrix} A \\ D \\ E \end{pmatrix} \begin{pmatrix} S \\ A \\ H \end{pmatrix} \begin{pmatrix} S \\ N \\ E \end{pmatrix} \begin{pmatrix} A \\ S \\ U \end{pmatrix} \begin{pmatrix} U \\ U \\ R \end{pmatrix} \begin{pmatrix} T \\ N \\ E \end{pmatrix} \xrightarrow{\text{diffusion en 3 points}} \begin{matrix} ADE SAH SNE \\ ASU UUR TNE \end{matrix}$$

Ce que l'on appelle un *algorithme de chiffrement*, ce sont les différentes techniques utilisées pour transformer le texte original. Quant à la *clé* de chiffrement, c'est, par exemple dans le cas du chiffre de César, le nombre de caractères de décalage (3 en l'occurrence), ou dans la technique de diffusion, le nombre de lignes des colonnes. La valeur de cette clé est variable, on aurait tout aussi bien décidé de faire des colonnes de 2 lignes, ou un décalage de 6 caractères.

Ce qui nous amène à la troisième grande idée : *le secret réside seulement dans la clé*. Après quelques millénaires, on s'est aperçu que c'était une mauvaise idée de partir du principe que personne n'arriverait à comprendre l'algorithme de chiffrement. Tôt ou tard, une personne finira bien par le découvrir... par la force si nécessaire.

De nos jours, l'algorithme peut donc être détaillé sur Wikipédia en long, en large et en travers, permettant à n'importe qui de vérifier qu'il n'a pas de point faible particulier, c'est-à-dire que la seule solution pour déchiffrer un texte sera de disposer de la *clé* qui a été employée avec celui-ci.

5.1.2 Vous voulez un dessin ?

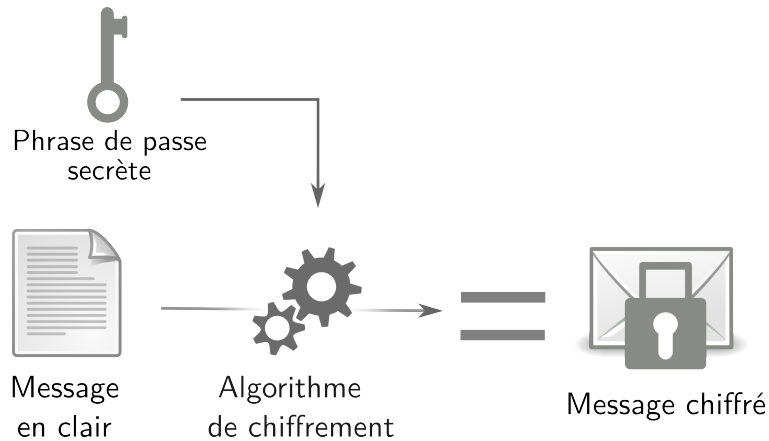
Concrètement, pour assurer la *confidentialité* de nos données, on utilise deux opérations : le chiffrement, puis le déchiffrement.

Première étape : le chiffrement

Pour un exemple d'usage pratique, prenons le message suivant³ :

2. Le passage qui suit est une adaptation très partielle de la [bande dessinée de Jeff Moser sur l'algorithme AES](http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html) [http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html] (en anglais).

3. Ce message est d'une très haute importance stratégique pour des personnes qu'on inviterait chez soi. Il est donc crucial de le chiffrer.



Les spaghetti sont dans le placard.

Après avoir chiffré ce message en utilisant le logiciel GnuPG avec l'algorithme AES256, et comme phrase de passe « *ceci est un secret* », on obtient :

-----BEGIN PGP MESSAGE-----

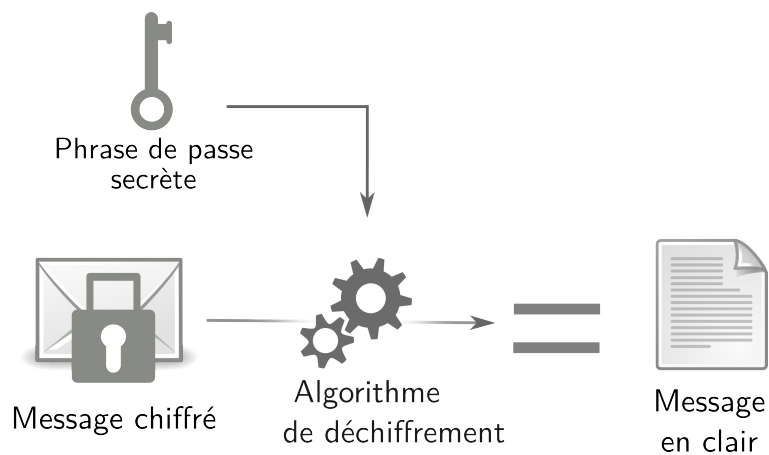
```
jA0ECQMCRM0lmTSI0NRg0lkBWGQI76cQ0ocEvdBhX6BM2AU6aYSPYymSqj8ihFXu
wV1GVraWuwEt4XnLc3F+0xT3EaXINMHdH9oydA92WDkaqPEnjsWQs/oSCeZ3WxOB
9mf9y6jzqozEHw==
=T6eN
```

-----END PGP MESSAGE-----

Voici donc l'aspect que prend un texte après chiffrement : son contenu est devenu parfaitement imbuvable. Les données « en clair », lisibles par tout le monde, ont été transformées en un autre format, incompréhensible pour qui ne possède pas la clé.

Deuxième étape : le déchiffrement

Pour le déchiffrement, il nous suffira d'utiliser de nouveau GnuPG, avec notre texte chiffré, cette fois. GnuPG nous demandera la phrase de passe ayant servi à chiffrer notre texte, et si cette dernière est correcte, on obtiendra enfin l'information qui nous manquait pour préparer le déjeuner.



5.1.3 Pour un disque dur...

Si on souhaite mettre sur un support de stockage (disque dur, clé USB, *etc.*) uniquement des données chiffrées, il va falloir que le système d'exploitation se charge de réaliser « à la volée » les opérations de chiffrement et de déchiffrement.

Ainsi, chaque fois que des données devront être lues du disque dur, elles seront déchiffrées au passage afin que les logiciels qui en ont besoin puissent y accéder. À l'inverse, chaque fois qu'un logiciel demandera à écrire des données, elles seront chiffrées avant d'atterrir sur le disque dur.

page 11

Pour que ces opérations fonctionnent, il est nécessaire que la clé de chiffrement se trouve en mémoire vive aussi longtemps que le support aura besoin d'être utilisé.

Par ailleurs, la clé de chiffrement ne peut pas être changée. Une fois que cette dernière a servi à chiffrer des données inscrites sur le disque, elle devient indispensable pour pouvoir les relire. Pour pouvoir changer la clé, il faudrait donc relire puis réécrire l'intégralité des données du disque...

Pour éviter cette opération pénible, la plupart des systèmes utilisés pour chiffrer les supports de stockage utilisent donc une astuce : la clé de chiffrement est en fait un grand nombre, totalement aléatoire, qui sera lui-même chiffré à l'aide d'une *phrase de passe*⁴. Cette version chiffrée de la clé de chiffrement est généralement inscrite sur le support de stockage au début du disque, « *en tête* » des données chiffrées.

Avec ce système, changer le code d'accès devient simple, vu qu'il suffira de remplacer uniquement cet *en-tête* par un nouveau.

5.1.4 Résumé et limites

tome 2 ch. 6

La cryptographie permet donc de bien protéger ses données⁵, en chiffrant tout ou partie de son disque dur comme de tout autre support de stockage (clé USB, CD, *etc.*), ou de ses communications. De plus, les ordinateurs modernes sont suffisamment puissants pour que nous puissions faire du chiffrement une routine, plutôt que de le réserver à des circonstances spéciales ou à des informations particulièrement sensibles (sinon, cela identifie tout de suite ces dernières comme importantes, alors qu'il vaut mieux les dissoudre dans la masse).

On peut ainsi mettre en place une phrase de passe pour chiffrer tout un disque dur, et/ou donner à certaines personnes une partie chiffrée avec leur propre phrase de passe. Il est également possible de chiffrer individuellement tel ou tel fichier, ou un email, ou une pièce jointe, avec une phrase de passe encore différente.

Cependant, bien qu'il soit un outil puissant et essentiel pour la sécurité des informations, **le chiffrement a ses limites** — en particulier lorsqu'il n'est pas utilisé correctement.

Comme expliqué auparavant, lorsqu'on accède à des données chiffrées, il est nécessaire de garder deux choses en tête. Premièrement, une fois les données déchiffrés, ces dernières se trouvent *au minimum* dans la mémoire vive. Deuxièmement, tant que des données doivent être chiffrées ou déchiffrées, la mémoire vive contient également la *clé de chiffrement*.

Toute personne qui dispose de la clé de chiffrement pourra lire *tout ce qui a été chiffré avec*, et aussi s'en servir pour chiffrer elle-même des données.

Il faut donc faire attention aux éléments suivants :

4. Le système LUKS, utilisé sous GNU/Linux, permet même d'utiliser plusieurs versions chiffrées de la clé de chiffrement. Chacune de ces versions pourra être chiffrée avec une *phrase de passe* différente, ce qui permet à plusieurs personnes d'accéder aux mêmes données sans pour autant avoir à retenir le même secret.

5. Un article en anglais sur un procès où la police avoue son impuissance face au chiffrement : Philip Willan, 2003, *PGP Encryption Proves Powerful* [<http://www.pcworld.com/article/110841/article.html>]

- Le système d'exploitation et les logiciels ont accès aux données et à la clé de chiffrement autant que nous, alors cela dépend de la confiance qu'on met en eux — encore une fois, il s'agit de ne pas installer n'importe quoi n'importe comment. [page 24]
- Quiconque obtient un accès physique à l'ordinateur allumé a, de fait, accès au contenu de la mémoire vive. Lorsqu'un disque chiffré est activé, celle-ci contient, en clair, les données sur lesquelles on a travaillé depuis l'allumage de l'ordinateur (même si elles sont chiffrées sur le disque). Mais elle contient surtout, comme dit plus haut, la clé de chiffrement, qui peut donc être copiée. Donc il vaut mieux s'habituer, quand on ne s'en sert pas, à éteindre les ordinateurs, et à désactiver (démonter, éjecter) les disques chiffrés. [page 19]
- Dans certains cas, il peut être nécessaire de prévoir des solutions matérielles pour pouvoir couper le courant facilement et rapidement⁶; ainsi les disques chiffrés redeviennent inaccessibles sans la phrase de passe — à moins d'effectuer une cold boot attack. [page 19]
- Il reste également possible qu'un enregistreur de frappe ait été installé sur l'ordinateur, et que celui-ci enregistre la phrase de passe. [page 26]

Par ailleurs, une certaine limite « légale » vient s'ajouter aux possibles attaques. En France, toute personne qui chiffre ses données est en effet censée donner le code d'accès aux autorités lorsqu'elles le demandent, comme l'explique l'*article 434-15-2 du Code Pénal*⁷ :

Est puni de trois ans d'emprisonnement et de 45 000 euros d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du code de procédure pénale.

Si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 75 000 euros d'amende.

À noter là-dedans : *susceptible* et *sur les réquisitions*. C'est-à-dire que la loi est assez floue pour permettre d'exiger de toute personne détentrice de données chiffrées qu'elle crache le morceau. On peut éventuellement se voir demander la phrase de passe d'un support qui ne serait pas le nôtre... et que nous n'aurions donc pas. On notera que personne, à notre connaissance, n'a pour l'instant jamais été condamné pour ça.

Enfin, il peut être judicieux de rappeler que les mathématiques utilisées dans les algorithmes cryptographiques ont parfois des défauts. Et beaucoup plus souvent encore, les logiciels qui les appliquent comportent des faiblesses. Certains de ces problèmes peuvent, du jour au lendemain, transformer ce qu'on pensait être la meilleure des protections en une simple affaire de « double clic »...

5.2 S'assurer de l'intégrité de données

Nous avons vu quelques pistes pour assurer la *confidentialité* de nos données. Toutefois, il peut être aussi important de pouvoir s'assurer de leur *intégrité*, c'est-à-dire de vérifier qu'elles n'aient pas subi de modification (par accident ou par malveillance).

⁶. Pour cette raison, il est de bon ton de ne pas laisser la batterie branchée dans un ordinateur portable quand elle n'est pas utilisée. Il suffit alors d'enlever le câble secteur pour l'éteindre.

⁷. Le terme légal est « cryptologie ». Une recherche sur ce mot sur [Légifrance \[http://www.legifrance.gouv.fr\]](http://www.legifrance.gouv.fr) donnera une liste exhaustive des textes de loi concernant ce domaine.

On peut également vouloir s'assurer de la provenance de nos données, en assurer l'*authenticité*.

Concrètement, après la lecture de ces pages, on peut comprendre à quel point il est complexe de s'assurer que les logiciels que l'on souhaite installer sur nos ordinateurs n'aient pas été modifiés en route afin d'y introduire des logiciels malveillants.

page 24

5.2.1 La puissance du hachoir

L'essentiel des techniques pour assurer l'intégrité ou l'authenticité reposent sur des outils mathématiques que la cryptographie a baptisés « fonctions de hachage ».

Ces dernières fonctionnent comme des *hachoirs*, capables de réduire n'importe quoi en tout petits morceaux. Et si notre hachoir fonctionne bien pour être utilisé en cryptographie, on sait que :

- avec les petits morceaux, impossible de reconstituer l'objet original sans essayer tous les objets de la terre ;
- le même objet, une fois passé au hachoir, donnera toujours les mêmes petits morceaux ;
- deux objets différents doivent donner des petits morceaux différents.

Lorsque ces propriétés sont réunies, il nous suffit alors de comparer les petits morceaux issus de deux objets pour savoir s'il étaient identiques.

Les petits morceaux qui sortent de notre hachoir s'appellent plus couramment une *somme de contrôle* ou une *empreinte*. Elle est généralement écrite sous une forme qui ressemble à :

f9f5a68a721e3d10baca4d9751bb27f0ac35c7ba

Vu que notre hachoir fonctionne avec des données de n'importe quelle taille et de n'importe quelle forme, comparer des empreintes peut nous permettre de comparer plus facilement des images, des CD, des logiciels, *etc.*

Notre hachoir n'est pas magique pour autant. On imagine tout de même bien qu'en réduisant n'importe quoi en petits cubes de taille identique, on peut se retrouver avec les mêmes petits cubes issus de deux objets différents. Cela s'appelle une *collision*. Ce carambolage mathématique n'est heureusement dangereux que lorsqu'il est possible de le provoquer... ce qui est déjà arrivé pour plusieurs fonctions de hachage après quelques années de recherche.

5.2.2 Vérifier l'intégrité d'un logiciel

Prenons un exemple : Alice a écrit un programme et le distribue sur des CD, que l'on peut trouver dans des clubs d'utilisateurs de GNU/Linux. Betty a envie d'utiliser le programme d'Alice, mais se dit qu'il aurait été très facile pour une administration mal intentionnée de remplacer un des CD d'Alice par un logiciel malveillant.

Elle ne peut pas aller chercher un CD directement chez Alice, qui habite dans une autre ville. Par contre, elle a rencontré Alice il y a quelque temps, et connaît sa voix. Elle lui téléphone donc, et Alice lui donne la *somme de contrôle* du contenu du CD :

CD d'Alice $\xrightarrow{\text{SHA}_{256}}$ $\begin{matrix} 94d93910609f65475a189d178ca6a45f \\ 22b50c95416afb1d8feb125dc3069d0 \end{matrix}$

Betty peut ensuite la comparer avec celle qu'elle génère à partir du CD qu'elle s'est procuré :

CD de Betty $\xrightarrow{\text{SHA256}}$ $\begin{matrix} 94d93910609f65475a189d178ca6a45f \\ 22b50c95416affb1d8feb125dc3069d0 \end{matrix}$

Comme les nombres sont les mêmes, Betty est contente, elle est sûre de bien utiliser le même CD que celui fourni par Alice.

Calculer ces sommes de contrôle ne leur prend pas beaucoup plus de temps que la lecture complète du CD... soit quelques minutes tout au plus.

Maintenant, mettons-nous dans la peau de Carole, qui a été payée pour prendre le contrôle de l'ordinateur de Betty à son insu. Pour cela, elle veut créer un CD qui ressemble à celui d'Alice, mais qui contient un logiciel malveillant.

Malheureusement pour elle, la fonction de hachage ne va que dans un sens. Elle doit donc commencer par se procurer le CD original d'Alice.

[page précédente]

Ensuite, elle modifie ce CD pour y introduire le logiciel malveillant. Cette première version ressemble de très près à l'original. Cela pourrait duper plus d'une personne qui ne ferait pas attention, mais elle sait que Betty vérifiera la somme de contrôle du CD qui lui permettra d'installer la nouvelle version.

Comme Alice utilise la fonction de hachage SHA256, qui n'a pas de défaut connu, il ne reste à Carole qu'à essayer un très grand nombre de variation des données de son CD, cela dans l'espoir d'obtenir une *collision*, c'est-à-dire la même somme de contrôle que celle d'Alice.

Malheureusement pour elle, et heureusement pour Betty, même avec de nombreux ordinateurs puissants, les chances de réussite de Carole dans un temps raisonnable (mettons, quelques années) sont extrêmement faibles.

Il suffit donc de se procurer une *empreinte*, ou *somme de contrôle*, par des intermédiaires de confiance pour vérifier l'*intégrité* de données. Tout l'enjeu est ensuite de se procurer ces empreintes par un moyen de confiance : de pouvoir vérifier leur *authenticité*...

5.2.3 Vérifier un mot de passe

Un autre exemple d'utilisation des fonctions de hachage concerne la vérification de l'*authenticité* d'une demande d'accès.

Si l'accès à un ordinateur est protégé par un mot de passe, comme l'ouverture d'une session sous GNU/Linux⁸, il faut que l'ordinateur puisse vérifier que le mot de passe est le bon. Mais les mots de passe ne sont pas enregistrés sur l'ordinateur, car il serait trop facile de les lire.

Mais alors comment l'ordinateur s'assure-t-il que le mot de passe tapé au clavier est exact ?

Lorsque l'on choisit un mot de passe pour son ordinateur, le système enregistre en fait, grâce à une fonction de hachage, une empreinte du mot de passe. Pour vérifier l'accès, il « hache » de la même manière le mot de passe que l'on a saisi. Et si les empreintes sont les mêmes, il considère que le mot de passe était le bon.

Il est donc possible de vérifier que le mot de passe correspond, sans garder le mot de passe lui-même !

5.3 Symétrique, asymétrique ?

Les techniques de chiffrement mentionnées jusqu'ici reposent sur une seule clé secrète, qui permet à la fois d'effectuer le chiffrement et le déchiffrement. On parle dans ce cas de cryptographie *symétrique*.

8. Rappelons-nous que ces mots de passe ne servent pas à protéger les données [page 31]!

Ceci en opposition avec la cryptographie *asymétrique* qui n'utilise pas la même clé pour chiffrer et déchiffrer. Autrement appelé « chiffrement à clé publique », ce dernier est surtout utilisé pour la communication « en ligne », on en parlera donc en détail dans le prochain tome.

[tome 2 ch. 6]

Une des propriétés les plus intéressantes de la cryptographie asymétrique que l'on peut évoquer brièvement est la possibilité de réaliser des *signatures numériques*. Comme son équivalent papier, une signature numérique permet d'apposer une marque de reconnaissance sur des données.

Ces signatures numériques utilisant la cryptographie asymétrique constituent la façon la plus simple de vérifier la provenance d'un logiciel. On sera donc amené à s'en servir plus loin...

01 001
100 0010
01
0000111
11100000 0000
00100010 1111
00011 00

00 0010
0000 0011 111
101 01010
1010001 111
000111011 100
101111010 0000
00001 11

0110 0010
10010 1011
011 0011
101010011 1101
101110011
101101 1110
0111 001

001
010 011
101 11 1011
000 100
00011 00
111001111 10100
110001111 111
00000101 100 1011
001 0100 1101 0010
110 0000
001 000100110 0011
1000000 0011 001110100 100
101 10 1010 011001
00 010
0000001
100000111 01010
110011000 1000
001110

10
000 1111
0111 100 000
000 01010
011011100
010001011 0011
0110000 1010
0010

1011 1001
1110 0011
0011 01001
01101100 010
101010001 1111
0010001 0010
1000 10

10
1100
111 010 1110
0111 1100
01010
01100011 0000
11000010 0101
01110110 00
0011

0011 1000
0010 1100
01111
01001100 010
111010000 10
1111110 0011
1100 00

DEUXIÈME PARTIE

Choisir des réponses adaptées

La panique s'est désormais emparée de nous. Tout ce qu'on fait sur un ordinateur nous trahit, jour après jour. Qui plus est lorsqu'on croit, à tort, « être en sécurité ».

Mais avant de retourner au pigeon voyageur et à la cache secrète derrière la bibliothèque, qu'on ouvre en tirant sur un faux livre (solutions rustiques à ne pas oublier totalement, ceci dit...), il y a un peu de marge. Pas tant que ça, mais tout de même.

C'est cette marge que ce texte s'appliquera dorénavant à cartographier.

Dans cette partie, c'est en expliquant quelques idées, tout aussi importantes qu'elles sont générales, que nous brosserons le tableau d'une méthodologie sommaire permettant à quiconque de répondre à la question suivante : *comment décider d'un ensemble de pratiques et d'outils adéquats à notre situation ?* Nous décrirons ensuite quelques situations-types, que nous nommons des *cas d'usage*, afin d'illustrer notre propos.

Évaluation des risques

Quand on se demande quelles mesures mettre en place pour protéger des données ou des communications numériques, on se rend assez vite compte qu'en la matière, on avance un peu à l'aveuglette.

D'abord parce que la plupart des solutions qu'on pourrait mettre en place ont aussi leurs inconvénients : parfois elles sont très pénibles à déployer, à entretenir ou à utiliser ; parfois on a le choix entre diverses techniques, dont aucune ne répond complètement au « cahier des charges » que l'on s'est fixé ; parfois elles sont bien trop nouvelles pour avoir l'assurance qu'elles fonctionnent réellement ; *etc.*

6.1 Que veut-on protéger ?

Dans le cadre de ce texte, ce qu'on veut protéger rentre en général dans la vaste catégorie de l'*information* : par exemple, le contenu de messages électroniques, des fichiers de données (photo, tracts, carnet d'adresses) ou l'existence même d'une correspondance entre telle et telle personne.

Le mot « protéger » recouvre différents besoins :

- **confidentialité** : cacher des informations aux yeux indésirables ;
- **intégrité** : conserver des informations en bon état, et éviter qu'elles ne soient modifiées sans qu'on s'en rende compte ;
- **accessibilité** : faire en sorte que des informations restent accessibles aux personnes qui en ont besoin.

Il s'agit donc de définir, pour chaque ensemble d'informations à protéger, les besoins de confidentialité, d'intégrité et d'accessibilité. Sachant que ces besoins entrent généralement en conflit, on réalise dès maintenant qu'il faudra, par la suite, poser des priorités et trouver des compromis entre eux : en matière de sécurité informatique, on a rarement le beurre et l'argent du beurre.

6.2 Contre qui veut-on se protéger ?

Rapidement, se pose la question des capacités des personnes qui en auraient après ce que l'on veut protéger. Et là, ça se corse, parce qu'il n'est pas facile de savoir ce que les personnes les plus qualifiées peuvent réellement faire, et de quels moyens et de quels budgets elles bénéficient. En suivant l'actualité, et par divers autres biais, on peut se rendre compte que cela varie beaucoup selon à qui on a affaire. Entre le gendarme du coin et la *National Security Agency* américaine, il y a tout un fossé sur les possibilités d'actions, de moyens et de techniques employées.

Par exemple, le chiffrement est un des moyens les plus adaptés pour éviter qu'une personne qui allumerait, déroberait ou saisirait judiciairement un ordinateur accède à

toutes les données qui y résident. Mais les lois en vigueur en France ont prévu le coup : dans le cadre d'une enquête, toute personne doit donner la clé de chiffrement afin de permettre aux enquêteurs d'avoir accès aux données, sans quoi elle risque des peines assez lourdes. Cette loi permet à des enquêteurs ayant peu de moyens techniques d'agir contre ce type de protection, même si en réalité, nous ne connaissons aucun cas où cette loi a été appliquée. En parallèle, des organismes disposent de plus de moyens, tels la NSA ou la DGSE, et rien n'est sûr concernant leurs possibilités. Quelle avance ont-ils dans le domaine du cassage de cryptographie ? Sont-ils au courant de failles dans certaines méthodes, qu'ils n'auraient pas dévoilées, et qui leur permettraient de lire les données ? Sur ces sujets, il n'y a évidemment aucun moyen d'être sûr de ce que ces entités peuvent faire, mais en même temps leur champ d'intervention est limité, et il y a peu de cas dans lesquels on risque d'être confronté à elles.

Un facteur important est aussi à prendre en compte : le coût. En effet, plus les moyens mis en place sont importants, plus les technologies utilisées sont complexes, et plus leur coût est élevé ; ça signifie qu'ils ne seront utilisés que dans des cas précis et tout aussi importants aux yeux des personnes concernées. Par exemple, il y a peu de chances de voir un ordinateur soumis à d'intenses tests dans de coûteuses expertises pour une affaire de vol à l'étalage.

Dès lors, avant même de chercher une solution, la question est de savoir qui pourrait tenter d'accéder à nos informations sensibles, afin de discerner s'il est nécessaire de chercher des solutions compliquées ou pas. Sécuriser complètement un ordinateur est de toutes façons de l'ordre de l'impossible, et dans cette histoire, il s'agit plutôt de mettre des bâtons dans les roues de celles et ceux qui pourraient en avoir après ce que l'on veut protéger. Plus l'on pense grands les moyens de ces personnes, plus les bâtons doivent être nombreux et solides.

Évaluer les risques, c'est donc avant tout se poser la question de quelles sont les données que l'on veut protéger, et de qui peut être intéressé par ces données. À partir de là, on peut avoir une vision de quels moyens ils disposent (ou en tout cas, dans la mesure du possible, essayer de se renseigner) et en conséquence, définir une *politique de sécurité* adaptée.

Définir une politique de sécurité

Une chaîne n'a que la solidité de son maillon le plus faible. Rien ne sert d'installer trois énormes verrous sur une porte blindée placée à côté d'une frêle fenêtre délabrée. De même, chiffrer une clé USB ne rime pas à grand-chose si les données qui y sont stockées sont utilisées sur un ordinateur qui en conservera diverses traces *en clair* sur son disque dur.

[page 37]

[page 19]

Ces exemples nous apprennent quelque chose : de telles « solutions » ciblées ne sont d'aucune utilité tant qu'elles ne font pas partie d'un ensemble de pratiques articulées de façon cohérente. Qui plus est, les informations qu'on veut protéger sont le plus souvent en relation avec des pratiques hors du champ des outils numériques. C'est donc de façon globale qu'il faut évaluer les risques et penser les réponses adéquates.

[page 49]

De façon globale, mais *située* : à une situation donnée correspond un ensemble singulier d'enjeux, de risques, de savoirs-faire... et donc de possibilités d'action. Il n'existe pas de solution miracle convenant à tout le monde, et qui réglerait tous les problèmes d'un coup de baguette magique. La seule voie praticable, c'est d'en apprendre suffisamment pour être capables d'imaginer et de mettre en place une politique de sécurité adéquate à sa propre situation.

7.1 Une affaire de compromis

On peut toujours *mieux* protéger ses données et ses communications numériques. Il n'y a de limite ni aux possibilités d'attaque et de surveillance, ni aux dispositifs qu'on peut utiliser pour s'en protéger. Cependant, à chaque protection supplémentaire qu'on veut mettre en place correspond un effort en termes d'apprentissage, de temps ; non seulement un effort initial pour s'y mettre, pour installer la protection, mais aussi, bien souvent, une complexité d'utilisation supplémentaire, du temps passé à taper des phrases de passe, à effectuer des procédures pénibles et répétitives, à porter son attention sur la technique plutôt que sur l'usage qu'on voudrait avoir de l'ordinateur.

Dans chaque situation, il s'agit donc de trouver un **compromis** convenable entre la facilité d'utilisation et le niveau de protection souhaité.

Parfois, ce compromis **n'existe** tout simplement **pas** : on doit parfois conclure que les efforts qui seraient nécessaires pour se protéger contre un risque plausible seraient trop pénibles, et qu'il vaut mieux courir ce risque... ou bien, tout simplement, ne pas utiliser d'outils numériques pour stocker certaines données ou pour parler de certaines choses. D'autres moyens existent, à l'efficacité prouvée de longue date : certains manuscrits de la Bible ont survécu des siècles durant, enfouis dans des jarres entreposées dans des grottes...

7.2 Comment faire ?

page 49

Il s'agit de répondre à la question suivante : quel ensemble de pratiques, d'outils me protégeraient de façon suffisante contre les risques évalués précédemment ?

Vous pouvez par exemple partir de vos pratiques actuelles, et vous mettre dans la peau de l'adversaire — aussi nauséabonde soit-elle — pour vous poser les questions suivantes :

1. Face à une telle politique de sécurité, quels sont les angles d'attaque les plus praticables ?
2. Quels sont les moyens à mettre en œuvre pour ce faire ?
3. Croyez-vous que ces moyens puissent être utilisés par les adversaires ?

Si vous répondez « oui » à la troisième question, prenez le temps de vous renseigner sur les solutions qui permettraient de vous protéger contre ces attaques, puis imaginez les modifications de pratiques entraînées par ces solutions et la politique de sécurité qui en découle. Si ça vous semble praticable, remettez-vous dans la peau de l'adversaire, et posez-vous à nouveau les questions énoncées ci-dessus.

Réitérez ce processus de réflexion, recherche et imagination jusqu'à trouver une voie praticable, un compromis tenable.

En cas d'incertitude, il est toujours possible de demander à une personne digne de confiance et plus compétente en la matière de se mettre dans la peau de l'adversaire : elle sera ravie de constater que vous avez fait vous-mêmes le gros du travail de réflexion, ce qui l'encouragera certainement à vous aider sur les points qui restent hors de votre portée.

7.3 Quelques règles

Avant de s'intéresser de plus près à l'étude de cas concrets et des politiques de sécurité qu'il serait possible de mettre en place, il existe quelques grands principes, quelques grandes familles de choix...

7.3.1 Complexe vs. simple

En matière de sécurité, une solution simple doit toujours être préférée à une solution complexe.

Tout d'abord, parce qu'une solution complexe offre plus de « surface d'attaque », c'est-à-dire plus de lieux où peuvent apparaître des problèmes de sécurité... ce qui ne manquera pas d'arriver.

Ensuite, parce que plus une solution est complexe, plus il faut de connaissances pour l'imaginer, la mettre en œuvre, la maintenir... mais aussi pour l'examiner, évaluer sa pertinence et ses problèmes. Ce qui fait qu'en règle générale, plus une solution est complexe, moins elle aura subi les regards acérés — et extérieurs — nécessaires pour établir sa validité.

Enfin, tout simplement, une solution complexe, qui ne tient pas en entier dans l'espace mental des personnes qui l'ont élaborée, a plus de chances de générer des problèmes de sécurité issus d'interactions complexes ou de cas particuliers difficiles à déceler.

Par exemple, plutôt que de passer des heures à mettre en place des dispositifs visant à protéger un ordinateur particulièrement sensible contre les intrusions provenant du réseau, autant l'en débrancher. On peut même parfois retirer physiquement la carte réseau...

page 13

7.3.2 Liste blanche, liste noire

Le réflexe courant, lorsqu'on prend connaissance d'une menace, est de chercher à s'en prémunir. Par exemple, après avoir découvert que tel logiciel laisse des traces de nos activités dans tel dossier, on nettoiera régulièrement cet emplacement. Jusqu'à découvrir que le même logiciel laisse aussi des traces dans un autre dossier, et ainsi de suite.

C'est le principe de la liste noire¹ : une liste des dossiers où sont enregistrés les fichiers temporaires, de logiciels qui envoient des rapports, *etc.* ; cette liste est complétée au fil des découvertes et des mauvaises surprises ; sur cette base, on essaie de faire au mieux pour se prémunir de chacune de ces menaces. Autrement dit, une liste noire fonctionne sur la base de la *confiance-sauf-dans-certains-cas*.

Le principe de la liste blanche est inverse, car c'est celui de la *méfiance-sauf-dans-certains-cas*. On interdit *tout, sauf* ce qu'on autorise explicitement. On interdit l'enregistrement de fichiers sur le disque dur, sauf à tel endroit, à tel moment. On interdit aux logiciels d'accéder au réseau, sauf certains logiciels bien choisis.

page 115

Voilà pour les principes de base.

Toute politique de sécurité basée sur le principe de la *liste noire* a un gros problème : une telle liste n'est jamais complète, car elle prend uniquement en compte les problèmes qui ont déjà été repérés. C'est une tâche sans fin, désespérante, que de tenir à jour une liste noire ; qu'on le fasse nous-mêmes ou qu'on le délègue à des gens ayant des connaissances informatiques pointues, quelque chose sera forcément oublié.

L'ennui, c'est que malgré leurs défauts réhivitoires, les outils basés sur une approche *liste noire* sont légion (comme nous allons le voir), au contraire de ceux s'appuyant sur la méthode *liste blanche*, qui nous est donc, sans doute, moins familière.

Mettre en œuvre l'approche *liste blanche* requiert donc un effort initial qui, s'il peut être important, est bien vite récompensé : apprendre à utiliser un système live qui n'écrit rien sur le disque dur sans qu'on lui demande, ça prend un temps non négligeable, mais une fois que c'est fait, c'en est fini des longues séances de nettoyage de disque dur, toujours à recommencer, et inefficaces car basées sur le principe de *liste noire*.

page 99

Une autre illustration nous est fournie par les logiciels antivirus, qui visent à empêcher l'exécution de programmes mal intentionnés. Vu qu'ils fonctionnent sur le principe de la liste noire, leurs bases de données doivent perpétuellement être mises à jour, systématiquement en retard. Une réponse à ce problème, avec l'approche liste blanche, est d'empêcher l'exécution de tout programme qui n'a pas été enregistré au préalable, ou de limiter les possibilités d'action de chaque programme ; ces techniques, nommées *Mandatory Access Control*, nécessitent aussi de maintenir des listes, mais il s'agit dans ce cas de listes *blanches*, et le symptôme d'une liste obsolète sera le dysfonctionnement d'un logiciel, plutôt que le piratage de l'ordinateur.

Aussi, il est bien plus intéressant de se donner les moyens, lorsque c'est possible, de s'appuyer sur des listes blanches les plus vastes possible, afin de pouvoir faire plein de choses chouettes avec des ordinateurs, dans une certaine confiance. Et de s'appuyer, quand la liste blanche adéquate n'existe pas, sur des listes noires solides, de provenance connue, en gardant en tête le problème intrinsèque à cette méthode ; listes noires qu'on aidera éventuellement à compléter, en partageant nos découvertes.

1. Les expressions « liste blanche » et « liste noire » peuvent évoquer une dimension raciste, que ce soient les termes en eux-mêmes, ou leur hiérarchisation. Cependant, il nous a semblé peu judicieux de ne pas utiliser les termes consacrés et actuellement utilisés par tous les programmes, modes d'emploi et autres documentations techniques.

7.3.3 On n'est pas des robots

Certaines pratiques très exigeantes peuvent être diablement efficaces... jusqu'à ce qu'on commette une erreur. Alors comme on finira forcément par en faire une, il vaut mieux les prévoir plutôt que de payer les pots cassés.

Par exemple, une clé USB destinée à n'être utilisée que sur des ordinateurs utilisant un système libre, et qu'on fait vraiment attention à ne pas laisser traîner, peut *quand même* finir par être oubliée sur une table... et être branchée sur Windows par une personne qui l'aura confondue avec une autre. Mais si elle a été formatée dès le départ avec un système de fichiers incompatible avec Windows, ça devrait limiter la casse...

[page 16]

Bref, on n'est pas des robots. Il vaut mieux se donner de solides garde-fous matériels, que de s'imposer une vigilance sans bornes — ça permet aussi de garder l'esprit tranquille.

7.3.4 Date limite de consommation

Une fois une politique de sécurité définie, il ne faut pas oublier de la revoir de temps en temps! Le monde de la sécurité informatique évolue très vite, et une solution considérée comme raisonnablement sûre à l'heure actuelle peut très bien être aisément attaquable l'an prochain.

N'oublions pas non plus de penser dans nos politiques de sécurité qu'il est important de surveiller la vie des logiciels dont on dépend : leurs problèmes, avec une incidence sur la sécurité, leurs mises à jour, avec parfois de bonnes ou de mauvaises surprises... Tout cela prend un peu de temps, et autant le prévoir dès le départ.

[page 169]

Cas d'usages

Trêve de théorie, illustrons maintenant ces notions avec quelques *cas d'usage* : à partir de situations données, nous indiquerons des pistes permettant de définir une politique de sécurité adéquate. Bon nombre des solutions techniques retenues seront expliquées dans la partie suivante, vers laquelle nous renverrons au besoin.

page 81

Vu qu'ils s'inscrivent tous dans le contexte hors-connexions de ce premier tome, ces cas d'usage auront quelque chose d'artificiel : ils partent tous du principe que les ordinateurs en jeu ne sont jamais connectés à des réseaux, et en particulier à Internet.

Cas d'usage : un nouveau départ, pour ne plus payer les pots cassés

*(ou comment faire le ménage sur un ordinateur
après des années de pratiques insouciantes)*

8.1 Contexte

Prenons un ordinateur utilisé sans précautions particulières pendant plusieurs années. Cette machine pose sans doute un ou plusieurs des problèmes suivants :

1. son disque dur conserve des traces indésirables du passé; [page 19]
2. le système d'exploitation est un logiciel propriétaire (exemple : Windows), et truffé de logiciels malveillants. [page 23]

Par ailleurs, des fichiers gênants y sont stockés de façon parfaitement transparente. En effet, cet ordinateur est utilisé pour diverses activités populaires, parmi lesquelles certaines, osons l'avouer, sont parfaitement légales, telles que :

- écouter de la musique et regarder des films pris sur Internet ;
- aider des sans-papiers à préparer leurs dossiers pour la préfecture ;
- dessiner une jolie carte de vœux pour Mamie ;
- fabriquer de menus faux papiers simplifiant grandement les démarches administratives (gonfler des fiches de paie, quand on en a marre de se voir refuser des locations, appart' après appart') ;
- tenir à jour la comptabilité familiale ;
- fabriquer des textes, musiques ou vidéos « terroristes » — plus précisément menaçant, selon la définition européenne du terrorisme¹, « de causer [...] des destructions massives [...] à une infrastructure [...] susceptible [...] de produire des pertes économiques considérables », « dans le but de [...] contraindre indûment des pouvoirs publics [...] à accomplir ou à s'abstenir d'accomplir un acte quelconque » ; par exemple, des employés de France Télécom qui, lors d'une lutte, menaceraient de mettre hors d'état de nuire le système de facturation, et d'ainsi permettre aux usagers de téléphoner gratuitement.

8.2 Évaluer les risques

8.2.1 Que veut-on protéger ?

Appliquons au cas présent les catégories définies lorsque nous parlions d'évaluation des risques : [page 49]

1. EUR-lex, 2002, *Décision-cadre 2002/475/JAI du Conseil de l'Union Européenne, relative à la lutte contre le terrorisme* [<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002F0475:FR:NOT>].

- confidentialité : éviter qu'un œil indésirable ne tombe trop aisément sur les informations stockées dans l'ordinateur ;
- intégrité : éviter que ces informations ne soient modifiées à notre insu ;
- accessibilité : faire en sorte que ces informations restent accessibles quand on en a besoin.

Ici, accessibilité et confidentialité sont prioritaires.

8.2.2 Contre qui veut-on se protéger ?

Cette question est importante : en fonction de la réponse qu'on lui donne, la politique de sécurité adéquate peut varier du tout au tout.

Geste généreux, conséquences judiciaires

Cet ordinateur pourrait être saisi lors d'une perquisition.

Par exemple, votre fils a généreusement donné un gramme de *shit* à un ami fauché, qui, après s'être fait pincer, a informé la police de la provenance de la chose... à la suite de quoi votre fils est pénalement considéré comme trafiquant de stupéfiants. D'où la perquisition.

Dans ce genre de cas, l'ordinateur a de grandes chances d'être examiné par la police, mettant en péril l'objectif de confidentialité. La gamme de moyens qui seront probablement mis en œuvre va du gendarme de Saint-Tropez, allumant l'ordinateur et cliquant partout, à l'expert judiciaire qui examinera de beaucoup plus près le disque dur ; il est en revanche improbable que des moyens extra-légaux, usuellement aux mains des services spéciaux et des militaires, soient utilisés dans cette affaire.

Cambriolage

Cet ordinateur pourrait être dérobé lors d'un cambriolage.

Au contraire de la police, les voleurs n'ont sans doute pas grand-chose à faire de vos petits secrets... et ne vous dénonceront pas. Au pire vous feront-ils chanter à propos de la récupération de vos données. Il est cependant improbable qu'ils mettent en œuvre de grands moyens pour les retrouver sur le disque dur de l'ordinateur.

8.3 Définir une politique de sécurité

Posez-vous maintenant, en vous mettant dans la peau de l'adversaire, les questions exposées dans notre méthodologie.

page 51

8.3.1 Première étape : quand ouvrir les yeux suffit pour voir

1. Angle d'attaque le plus praticable : brancher le disque dur sur un autre ordinateur, examiner son contenu, y trouver tous vos petits secrets.
2. Moyens nécessaires : un autre ordinateur, dont le gendarme de Saint-Tropez se servira pour trouver le plus gros de vos secrets ; un expert judiciaire, lui, saurait aussi retrouver les fichiers que vous croyiez avoir effacés ; Nostradamus en déduirait la date de levée de vos semis.
3. Crédibilité de l'attaque : grande.

page 37

Il faut donc adapter vos pratiques. Contre ce type d'attaque, chiffrer le disque dur est la réponse évidente : installer et utiliser un système chiffré est désormais relativement simple.

page 105

Les étapes pour y arriver seraient alors :

1. Lancer un système *live* afin d'effectuer les opérations suivantes dans un contexte relativement sûr :
 - sauvegarder temporairement, sur un disque externe ou une clé USB chiffrés, les fichiers qui doivent survivre au grand nettoyage ;
 - éjecter/démonter et débrancher ce support de stockage externe ;
 - effacer « pour de vrai » l'intégralité du disque dur **interne** de l'ordinateur.
2. Installer un système d'exploitation libre, en précisant au programme d'installation de chiffrer le disque dur, mémoire virtuelle (*swap*) comprise. [page 17]
3. Recopier vers le nouveau système les données préalablement sauvegardées.
4. Mettre en place ce qu'il faut pour supprimer des fichiers de façon « sécurisée », afin de pouvoir...
5. Effacer le contenu des fichiers qui se trouvent sur le support de sauvegarde temporaire, qui pourra éventuellement resservir.

Et ensuite, de temps à autre, faire en sorte que les données supprimées sans précautions particulières ne soient pas récupérables par la suite. Il faudra également veiller à mettre régulièrement à jour le système, afin de combler les « trous de sécurité » que pourraient utiliser des logiciels malveillants. [page 24]

Pour effectuer ces étapes, se référer aux recettes suivantes :

- chiffrer un disque externe ou une clé USB, voir page 137 ;
- utiliser un système *live*, voir page 99 ;
- sauvegarder des données, voir page 143 ;
- effacer « pour de vrai », voir page 127 ;
- installer un système chiffré, voir page 105 ;
- garder un système à jour, voir page 169.

Cette voie semblant praticable, posons-nous, de nouveau, les mêmes questions.

8.3.2 Seconde étape : le tiroir de la commode n'était pas chiffré

1. Angle d'attaque : l'équivalent des fichiers qu'on cherche à protéger traîne peut-être dans la pièce voisine, dans le troisième tiroir de la commode, sur papier ou sur une clé USB.
2. Moyens nécessaires : perquisition, cambriolage, ou autre visite impromptue.
3. Crédibilité de l'attaque : grande, c'est précisément contre ce type de situations qu'on cherche à se protéger ici.

Là encore, on constate qu'une politique de sécurité doit être pensée comme un tout. Sans un minimum de cohérence dans les pratiques, rien ne sert de s'embêter à taper des phrases de passe longues comme un jour sans pain. [page 51]

Il est donc temps de trier les papiers dans la commode, et de nettoyer toute clé USB, CD, DVD contenant des données qu'on compte désormais chiffrer :

- sauvegarder sur un support chiffré les données à conserver
- pour les clés USB et disques durs externes : effacer pour de vrai leur contenu ; [page 127]
- pour les CD et DVD : les détruire, et se débarrasser des résidus ;
- décider que faire des données préalablement sauvegardées : les recopier sur le disque dur nouvellement chiffré ou les archiver. [page 77]

8.3.3 Troisième étape : la loi comme moyen de coercition

1. Angle d'attaque : la police a le droit d'exiger que vous lui donniez accès aux informations chiffrées, comme expliqué dans le chapitre consacré à la cryptographie. [page 37]
2. Moyens nécessaires : suffisamment de persévérance dans l'enquête pour appliquer cette loi.

3. Crédibilité de l'attaque : encore faut-il que la police considère pouvoir trouver des éléments à charge sur l'ordinateur, avec suffisamment de foi pour pousser le bouchon jusque-là. Dans le strict cadre de l'enquête qui part du gramme de *shit*, c'est peu probable, mais pas du tout impossible.

Si la police en arrive à exiger l'accès aux données chiffrées, se posera, en pratique, la question suivante : les informations contenues dans l'ordinateur font-elles encourir plus de risques que le refus de donner la phrase de passe ? Après, c'est selon comment on le sent. Céder, dans cette situation, ne remet pas en cause tout l'intérêt de chiffrer, au départ, son disque dur : ça permet tout au moins de savoir ce qui a été dévoilé, quand, et à qui.

Ceci dit, il peut être bon de s'organiser pour vivre de façon moins délicate une telle situation : le nouvel objectif pourrait être d'avoir un disque dur suffisamment « propre » pour que ce ne soit pas la catastrophe si on cède face à la loi, ou si le système cryptographique utilisé est cassé.

page 77

Comme premier pas, il est souvent possible de faire un compromis concernant l'accessibilité, pour des fichiers concernant des projets achevés dont on n'aura pas besoin souvent ; on traitera ceci dans le cas d'usage sur l'archivage, qu'il pourra être bon d'étudier après celui-ci.

Ensuite, c'est toute la question de la compartimentation qui se pose ; en effet, s'il est possible d'augmenter globalement, de nouveau, le niveau de sécurité de l'ensemble des activités pratiquées... ce serait trop pénible à l'usage. Il convient donc de préciser les besoins respectifs, en termes de confidentialité, de ces diverses activités. Et, à partir de là, faire le tri et décider lesquelles, plus « sensibles » que les autres, doivent bénéficier d'un traitement de faveur.

page 65

Le prochain cas d'usage étudiera de tels traitements de faveur, mais patience, mieux vaut pour l'instant terminer la lecture de celui-ci !

8.3.4 Quatrième étape : en réseau

tome 2 § 3.4

Tout ceci est valable pour un ordinateur hors-ligne. D'autres angles d'attaques sont imaginables, s'il est connecté à un réseau. Le second tome de ce guide les étudiera.

Et au-delà de ces problèmes, plusieurs autres angles d'attaque demeurent encore envisageables contre une telle politique de sécurité.

8.3.5 Angle d'attaque : une brèche dans le système de chiffrement utilisé

Comme il a déjà été expliqué en ces pages, tout système de sécurité finit par être cassé. Si l'algorithme de chiffrement utilisé est cassé, ça fera la une des journaux, tout le monde sera au courant, et il sera possible de réagir.

Mais si c'est sa mise en œuvre dans le noyau Linux qui est cassée, ça ne passera pas dans *Libération*, et il y a fort à parier que seuls les spécialistes de la sécurité informatique seront au courant.

Lorsqu'on ne côtoie pas de tels êtres, une façon de se tenir au courant est de s'abonner aux annonces de sécurité de Debian². Les emails reçus par ce biais sont rédigés en anglais, mais ils donnent l'adresse de la page où on peut trouver leur traduction française. La difficulté, ensuite, est de les interpréter...

². La liste de diffusion se nomme `debian-security-announce` [<http://lists.debian.org/debian-security-announce/>].

Ceci étant dit, même si le système de chiffrement utilisé est « cassé », encore faut-il que les adversaires le sachent... le gendarme de Saint-Tropez n'en saura rien, mais un expert judiciaire, si.

Par ailleurs, dans le rayon science-fiction, rappelons qu'il est difficile de connaître l'avance qu'ont, en la matière, militaires et agences gouvernementales — comme la NSA.

8.3.6 Angle d'attaque : *cold boot attack*

1. Angle d'attaque : la *cold boot attack* est décrite dans le chapitre consacré aux traces.
2. Moyens nécessaires : accéder physiquement à l'ordinateur pendant qu'il est allumé ou éteint depuis peu, par exemple lors d'une perquisition.
3. Crédibilité de l'attaque : à notre connaissance, cette attaque n'a jamais été utilisée, du moins de façon publique, par des autorités. Sa crédibilité est donc très faible.

page 19

Il peut sembler superflu de se protéger contre cette attaque dans la situation décrite ici, mais mieux vaut prendre, dès maintenant, de bonnes habitudes, plutôt que d'avoir de mauvaises surprises dans quelques années. Quelles habitudes ? En voici quelques-unes qui rendent plus difficile cette attaque :

- éteindre l'ordinateur lorsqu'on ne s'en sert pas ;
- prévoir la possibilité de couper le courant facilement et rapidement : interrupteur de multiprise aisément accessible, ôter la batterie d'un ordinateur portable quand il est branché sur le secteur (... il suffit alors de débrancher le cordon secteur pour éteindre la machine) ;
- rendre l'accès au compartiment de votre ordinateur contenant la RAM plus long et difficile, par exemple en le collant/soudant.

8.3.7 Angle d'attaque : l'œil et la vidéo-surveillance

Avec le système chiffré imaginé à la première étape, la confidentialité des données repose sur le fait que la phrase de passe soit gardée secrète. Si elle est tapée devant une caméra de vidéo-surveillance, un adversaire ayant accès à cette caméra ou à ses éventuels enregistrements pourra découvrir ce secret, puis se saisir de l'ordinateur et avoir accès aux données. Plus simplement, un œil attentif, dans un bar, pourrait voir la phrase de passe pendant qu'elle est tapée.

Monter une telle attaque nécessite de surveiller les personnes utilisant cet ordinateur, jusqu'à ce que l'une d'entre elles tape la phrase de passe au mauvais endroit. Ça peut prendre du temps et c'est coûteux.

Dans la situation décrite ici, une telle attaque relève de la pure science-fiction ; à l'heure actuelle, rares sont les organisations susceptibles de mettre en œuvre des moyens aussi conséquents, mis à part divers services spéciaux : anti-terroristes, espionnage industriel...

Pour se prémunir d'une telle attaque, il convient de :

- choisir une longue phrase de passe, qui rend impossible la mémorisation « à la volée » par un observateur humain ;
- vérifier autour de soi, à la recherche d'éventuels yeux (humains ou électroniques) indésirables, avant de taper sa phrase de passe.

page 91

8.3.8 Angle d'attaque : la partie non-chiffrée et le micrologiciel

Comme expliqué dans la recette dédiée, un système « chiffré » ne l'est pas entière-

page 105

ment : le petit logiciel qui nous demande, au démarrage, la phrase de passe de chiffrement du *reste* des données, est, lui, stocké en clair sur la partie du disque dur qu'on nomme `/boot`. Un attaquant ayant accès à l'ordinateur peut aisément, en quelques minutes, modifier ce logiciel, y installer un *keylogger*, qui conservera la phrase de passe, pour venir la chercher plus tard, ou, tout simplement, l'enverra par le réseau.

page 23

Si cette attaque est montée à l'avance, l'adversaire pourra déchiffrer le disque dur quand il se saisira de l'ordinateur, lors d'une perquisition par exemple.

Les moyens nécessaires pour cette attaque sont, somme toute, assez limités : *a priori*, point n'est besoin d'être Superman pour avoir accès, pendant quelques minutes, à la pièce où réside l'ordinateur.

Cependant, là aussi, dans la situation décrite pour ce cas d'usage, nous sommes en pleine science-fiction. Mais la réalité a parfois tendance à dépasser la fiction...

La seule protection praticable contre cette attaque est de stocker les programmes de démarrage, dont ce petit dossier non-chiffré (`/boot`), sur un support externe, comme une clé USB, qui sera conservé en permanence dans un endroit plus sûr que l'ordinateur. C'est l'*intégrité* de ces données, et non leur *confidentialité*, qui est alors à protéger. Cette pratique exige pas mal de compétences et de rigueur ; nous ne la développerons pas dans ce guide.

De telles pratiques mettent la barre plus haut, mais il reste un mais : une fois obtenu l'accès physique à l'ordinateur, si `/boot` n'est pas accessible, et donc pas modifiable, il reste possible d'effectuer le même type d'attaque sur le micrologiciel de la machine. C'est légèrement plus difficile, car la façon de faire dépend du modèle d'ordinateur utilisé, mais c'est possible. Nous ne connaissons aucune façon praticable de s'en protéger.

8.3.9 Angle d'attaque : les logiciels malveillants

page 23

Nous avons appris dans un chapitre précédent que des logiciels installés à notre insu sur un ordinateur peuvent nous dérober des données. Dans le cas présent, un tel logiciel est en mesure de transmettre la clé de chiffrement du disque dur à un adversaire... qui obtiendra ensuite, grâce à cette clé, l'accès aux données chiffrées, quand il aura accès physique à l'ordinateur.

Installer un logiciel malveillant sur le système Debian dont il est question ici requiert des compétences de plus haut niveau que les attaques étudiées ci-dessus, mais aussi plus de préparation. Une telle attaque relève donc, ici aussi, de la science-fiction, du moins en ce qui concerne la situation qui nous occupe. Dans d'autres situations, il conviendra parfois d'être extrêmement prudent quant à la provenance des données et logiciels qu'on injecte dans l'ordinateur, en particulier lorsqu'il est connecté à Internet... un cas qui, rappelons-le, n'est pas notre propos dans ce premier tome.

page 117

La recette concernant l'installation de logiciels donne quelques pistes fort utiles sur la façon d'installer de nouveaux logiciels proprement. Le second tome de ce guide, consacré aux réseaux, et à Internet en particulier, prolonge cette étude.

8.3.10 Angle d'attaque : la force brute

Attaquer un système cryptographique par « force brute » est la plus simple, la plus stupide, et la plus lente des manières. Mais quand on ne peut mettre en œuvre un autre type d'attaque...

Pour le disque dur chiffré lors de l'étape 1, ça demande énormément de temps (de nombreuses années) et/ou énormément d'argent et des compétences pointues... du moins si la phrase de passe est solide.

Ce qu'on peut se dire, c'est qu'*a priori*, si une organisation est prête à mobiliser autant de ressources pour avoir accès à vos données, elle gagnerait amplement à mettre en place une des autres attaques, moins coûteuses et tout aussi efficaces, listées ci-dessus.

Cas d'usage : travailler sur un document sensible

9.1 Contexte

Après avoir pris un nouveau départ, l'ordinateur utilisé pour mener ce projet à bien a été équipé d'un système chiffré. Bien. Survient alors le besoin de travailler sur un projet particulier, plus « sensible », par exemple :

[page 57]
[page 105]

- un tract doit être rédigé ;
- une affiche doit être dessinée ;
- un livre doit être maqueté puis exporté en PDF ;
- une fuite d'informations doit être organisée pour divulguer les affreuses pratiques d'un employeur ;
- un film doit être monté et gravé sur DVD.

Dans tous ces cas, les problèmes à résoudre sont à peu près les mêmes.

Comme il serait trop pénible d'augmenter globalement, de nouveau, le niveau de sécurité de l'ordinateur, il est décidé que ce projet particulier doit bénéficier d'un traitement de faveur.

9.1.1 Conventions de vocabulaire

Par la suite, nous nommerons :

- les *fichiers de travail* : l'ensemble des fichiers nécessaires à la réalisation de l'œuvre : les images ou *rushes* utilisés comme bases, les documents enregistrés par le logiciel utilisé, *etc.* ;
- l'*œuvre* : le résultat final (tract, affiche, *etc.*)

En somme, la matière première, et le produit fini.

9.2 Évaluer les risques

Partant de ce contexte, tentons maintenant de définir les risques auxquels exposent les pratiques décrites dans ce cas d'usage.

9.2.1 Que veut-on protéger ?

Appliquons au cas présent les catégories définies lorsque nous parlions d'évaluation des risques :

[page 49]

- confidentialité : éviter qu'un œil indésirable ne découvre trop aisément l'œuvre et/ou les fichiers de travail ;

- intégrité : éviter que ces documents ne soient modifiés à notre insu ;
- accessibilité : faire en sorte que ces documents restent accessibles quand on en a besoin.

Ici, accessibilité et confidentialité sont prioritaires.

Accessibilité, car l'objectif principal est tout de même de réaliser l'œuvre. S'il fallait se rendre au pôle Nord pour ce faire, le projet risquerait fort de tomber à l'eau.

Et pour ce qui est de la confidentialité, tout dépend de la publicité de l'œuvre. Voyons donc ça de plus près.

Œuvre à diffusion restreinte

Si le contenu de l'œuvre n'est pas complètement public, voire parfaitement secret, il s'agit de dissimuler à la fois l'œuvre *et* les fichiers de travail.

Œuvre diffusée publiquement

Si l'œuvre a vocation à être publiée, la question de la confidentialité se ramène à celle de l'anonymat.

C'est alors, principalement, les fichiers de travail qui devront passer sous le tapis : en effet, les découvrir sur un ordinateur incite fortement à penser que ses propriétaires ont réalisé l'œuvre... avec les conséquences potentiellement désagréables que cela peut avoir.

Mais ce n'est pas tout : si l'œuvre, ou ses versions intermédiaires, sont stockées sur cet ordinateur (PDF, *etc.*), leur date de création est très probablement enregistrée dans le système de fichiers et dans des méta-données. Le fait que cette date soit antérieure à la publication de l'œuvre peut aisément amener des adversaires à tirer des conclusions gênantes quant à sa généalogie.

page 16
page 21

9.2.2 Contre qui veut-on se protéger ?

Pour faire simple, reprenons les possibilités décrites dans le cas d'usage « un nouveau départ » : l'ordinateur utilisé pour réaliser l'œuvre peut être dérobé, plus ou moins fortuitement, par de quelconques flics, voire par de braves voleurs travaillant à leur compte.

page 57

9.3 Accro à Windows ?

La première question qui se pose est : quel système d'exploitation utiliser ? Ça dépend, évidemment, des logiciels utilisés pour ce projet :

S'ils fonctionnent sous GNU/Linux, continuons la lecture de ce chapitre pour étudier les options qui s'offrent à nous.

S'ils fonctionnent exclusivement sous Windows, c'est dommage. Mais nous étudions tout de même un chemin praticable qui permet de limiter la casse. Allons donc voir à quoi ressemble ce chemin, en ignorant les paragraphes suivants, qui sont consacrés à GNU/Linux.

page 68

9.4 Le système *live* amnésique

Les problèmes attendant à la situation de départ sont les mêmes que ceux du cas d'usage « un nouveau départ ». Mais avant de mettre sur la table de potentielles politiques de sécurité, lançons-nous dans un rapide tour d'horizon des outils et méthodes disponibles.

page 57

9.4.1 Liste noire vs. liste blanche

Vu qu'on a déjà un système Debian chiffré, on peut, de prime abord, imaginer le configurer finement pour qu'il conserve moins de traces de nos activités sur le disque dur. Le problème de cette approche, c'est qu'elle est de type « liste noire », et nous en avons expliqué les limites en ces pages : quel que soit le temps consacré, quelle que soit l'expertise mise au travail, même avec une compréhension particulièrement poussée des entrailles du système d'exploitation utilisé, on oubliera toujours une petite option bien cachée, il restera toujours des traces indésirables auxquelles on n'avait pas pensé.

[page 53]

Au contraire, certains systèmes *live* fonctionnent sur le principe de la « liste blanche » : tant qu'on ne le demande pas explicitement, aucune trace n'est laissée sur le disque dur.

[page 99]

En envisageant uniquement le critère « confidentialité », le système *live* bat donc l'autre à plate couture. En termes de temps et de difficulté de mise en œuvre, en revanche, la comparaison est plus mitigée.

9.4.2 Le beurre, ou l'argent du beurre ?

Un système *live* est en effet amnésique ; c'est certes son principal atout, mais cette propriété est aussi source d'inconvénients. Par exemple, dans le cas où notre système *live* préféré ne fournit pas un logiciel donné, qui est pourtant indispensable au projet, il faut, au choix :

- installer le logiciel dans le système *live* au début de chaque session de travail ;
- créer une clé *live* incluant notre logiciel dans son volume persistant ;
- faire du lobbying auprès des auteurs du système *live* pour qu'ils y ajoutent le logiciel souhaité ;

L'utilisation d'un système *live* est la solution la plus sûre et, dans ce cas, la moins difficile à mettre en place. Auquel cas, allons étudier une politique de sécurité basée là-dessus.

[page suivante]

À noter qu'il est possible d'installer une Debian dans VirtualBox, mais cette solution est réservée aux utilisateurs avertis, et ne sera donc pas documentée ici.

9.5 Travailler sur un document sensible... sur un système *live*

[page 65] Après avoir présenté le contexte dans le début de ce cas d'usage, et avoir décidé d'utiliser un système *live*, reste à mettre cette solution en place... et à étudier ses limites.

9.5.1 Télécharger et installer le système *live*

Tous les systèmes *live* ne sont pas particulièrement destinés à des pratiques « sensibles ». Il importe donc de choisir un système spécialement conçu pour (tenter de) ne laisser aucune trace sur le disque dur de l'ordinateur sur lequel il est utilisé.

[page 100] Si l'on ne dispose pas encore d'une copie de la dernière version du système *live Tails*, suivre la recette télécharger et installer un système *live* « discret ».

[page 93] À partir du premier périphérique *Tails* ainsi créé, nous allons créer une clé USB dédiée à notre projet. Pour cela démarrer le système *live* précédemment installé puis suivre les recettes cloner une clé *Tails* puis créer et configurer un volume persistant dans *Tails* en activant uniquement l'option *Données personnelles*.
[page 101]

[page 102]

9.5.2 Installer un éventuel logiciel additionnel

[page 103] Si l'on a besoin d'utiliser un logiciel qui n'est pas installé dans *Tails* et que l'on ne veut pas le réinstaller à chaque fois, suivre la recette installer un logiciel additionnel persistant dans *Tails*.

9.5.3 Utiliser le système *live*

[page 93] Chaque fois que l'on souhaite travailler sur notre document, il suffira de démarrer sur la clé contenant notre système *live* et sa persistance chiffrée puis d'activer le volume persistant.
[page 102]

9.5.4 Supprimer le système *live*

[tome 2 ch. 9] Une fois notre projet terminé et imprimé ou publié en ligne, il nous faut supprimer le volume persistant après avoir éventuellement archivé le projet

[page 102]

9.5.5 Limites

[plus bas] Certaines limites, communes à cette méthode et à celle basée sur l'usage de Windows, sont exposées plus loin.

[page 75]

9.6 Travailler sur un document sensible... sous Windows

[page 65] Après avoir présenté le contexte dans le début de ce cas d'usage et décidé, malgré tous les problèmes que ça pose, d'utiliser Windows, essayons maintenant de trouver une façon de limiter quelque peu la casse.

9.6.1 Point de départ : une passoire et une boîte de rustines desséchées

Partons d'un ordinateur muni, de la façon la plus classique qui soit, d'un disque dur sur lequel Windows est installé. Nous ne nous appesantirons pas sur cette situation, la première partie de cet ouvrage ayant abondamment décrit les multiples problèmes qu'elle pose. Une passoire, en somme, pleine de trous de sécurité.

On peut donc imaginer coller quelques rustines sur cette passoire. Faisons-en rapidement le tour.

Un disque dur, ça se démonte et ça se cache. Certes. Mais il y a les périodes où l'on s'en sert, parfois plusieurs jours ou semaines d'affilée. Cette rustine est basée sur deux hypothèses quelque peu osées :

- *Nous avons de la chance.* Il suffit en effet que l'accident (perquisition, cambriolage, etc.) survienne au mauvais moment pour que toute la confidentialité désirée soit réduite à néant ;
- *Notre discipline est parfaitement rigoureuse.* En effet, si l'on oublie, ou qu'on ne prend pas le temps, d'aller « ranger » le disque dur quand on n'en a plus besoin, et que l'accident survient à ce moment-là, c'est perdu, fin de la partie.

Par ailleurs, des outils existent pour chiffrer des données sous Windows. Quelle que soit la confiance qu'on leur accorde, il n'en reste pas moins qu'ils s'appuient obligatoirement sur les fonctions offertes par la boîte noire qu'est Windows. On ne peut donc que s'en méfier, et dans tous les cas, Windows, lui, aura accès à nos données *en clair*, et personne ne sait ce qu'il pourrait bien en faire.

Pour conclure ce petit tour dans la cour des miracles douteux, ajoutons que la seule « solution » possible dans le cas présent serait une approche de type liste noire, dont l'inefficacité crasse a déjà été expliquée précédemment.

page 51

Il est maintenant temps de passer aux choses sérieuses.

9.6.2 Seconde étape : enfermer Windows dans un compartiment (presque) étanche

Ce qui commence à ressembler à une solution sérieuse, ce serait de faire fonctionner Windows dans un compartiment étanche, dans lequel on ouvrirait, quand c'est nécessaire et en connaissance de cause, une porte pour lui permettre de communiquer avec l'extérieur de façon strictement limitée.

En d'autres termes, mettre en place une solution basée sur une logique de type *liste blanche* : rien ne pourrait entrer dans Windows ou en sortir *a priori*, et à partir de cette règle générale, on autorise des *exceptions*, au cas par cas, en réfléchissant à leur impact.

La *virtualisation*¹ permet de mettre en place ce type de systèmes. C'est un ensemble de techniques matérielles et logicielles qui permettent de faire fonctionner, sur un seul ordinateur, plusieurs systèmes d'exploitation, séparément les uns des autres, (presque) comme s'ils fonctionnaient sur des machines physiques distinctes.

Il est ainsi relativement facile, de nos jours, de faire fonctionner Windows à l'intérieur d'un système GNU/Linux, en lui coupant, par la même occasion, tout accès au réseau — et en particulier, en l'isolant d'Internet.



Attention : il est conseillé de lire l'intégralité de ce chapitre **avant** de se précipiter sur les recettes pratiques ; la description de l'hypothèse qui suit est assez longue, et ses limites sont étudiées à la fin de ce chapitre, où des contre-mesures sont envisagées. Il serait quelque peu dommage de passer quatre heures à suivre ces recettes, avant de se rendre compte qu'une toute autre solution serait, en fait, plus adéquate.

Commençons par résumer l'hypothèse proposée.

L'idée est donc de faire fonctionner Windows dans un compartiment *a priori* étanche, à l'intérieur d'un système Debian chiffré tel que celui qui a pu être mis en place à la suite de la lecture du cas d'usage précédent. Ce qui servira de disque dur à Windows, c'est en fait un gros fichier, rangé à côté de tous nos autres fichiers, sur le disque dur de notre système Debian chiffré. Ce fichier, qui n'a vraiment rien de particulier, nous le nommons une *image de disque virtuel*, parfois abrégé par une *image de disque*.

page 57

1. Pour plus d'informations, voir la page Wikipédia, 2014, *Virtualisation* [<https://fr.wikipedia.org/wiki/Virtualisation>].

Le fait que ce pseudo-disque dur soit un fichier nous simplifiera grandement la vie par la suite, qui décrit plus précisément la procédure envisagée.

Installer VirtualBox

page 156

La recette « installer Virtual Box » explique comment installer le logiciel VirtualBox, qui nous servira à lancer Windows dans un compartiment étanche.

Installer un Windows « propre » dans VirtualBox

page 157

Préparons une image de disque virtuel *propre* : la recette « installer un Windows virtualisé » explique comment installer Windows dans VirtualBox en lui coupant, **dès le départ**, tout accès au réseau.

À partir de ce moment-là, on qualifie Windows de système *invité* par le système Debian chiffré, qui, lui, est le système *hôte*.

Installer les logiciels nécessaires dans le Windows « propre »

Autant installer, dès maintenant, dans le Windows « propre », tout logiciel *non compromettant*² nécessaire à la réalisation des œuvres préméditées : ça évitera de le refaire au début de chaque nouveau projet... et ça évitera, souhaitons-le ardemment, d'utiliser une image Windows « sale » pour un nouveau projet, un jour où le temps presse.

Vu que le Windows *invité* n'a pas le droit de sortir de sa boîte pour aller chercher lui-même des fichiers, il est nécessaire de lui faire parvenir depuis « l'extérieur » les fichiers d'installation des logiciels nécessaires.

Une telle opération sera aussi utile, par la suite, pour lui envoyer toutes sortes de fichiers, et nous y reviendrons. Pour l'heure, vu que nous sommes en train de préparer une image de Windows « propre », servant de base à chaque nouveau projet, ne mélangeons pas tout, et contentons-nous de lui envoyer uniquement ce qui est nécessaire à l'installation des logiciels non compromettants souhaités.

Créons, sur le système hôte, un dossier nommé *Logiciels Windows*, et copions-y **uniquement** les fichiers nécessaires à l'installation des logiciels souhaités.

page 164

Puis partageons ce dossier avec le Windows *invité*, sans rendre ce partage permanent ; la recette « envoyer des fichiers au système virtualisé » explique comment procéder pratiquement.

Et en ce qui concerne l'installation des logiciels à l'intérieur du Windows *invité* : toute personne suffisamment accro à Windows pour lire ces pages est, sans aucun doute, plus compétente que celles qui écrivent ces lignes.



Attention : une fois cette étape effectuée, il est impératif de ne **rien** faire d'autre dans ce Windows virtualisé.

Congeler le Windows « propre »

Congelons maintenant l'image de disque *propre* qui vient d'être préparée, c'est-à-dire : sauvegardons-la dans un coin, telle quelle, et on ne démarrera plus **jamais** dessus. Par la suite, elle ne servira plus que de base de départ.

page 160

La recette sauvegarder une image de disque virtuel explique comment effectuer cette opération.

2. S'il est nécessaire de cacher qu'on fabrique des films, avoir des logiciels de montage vidéo peut être compromettant, parce qu'il serait plus difficile de nier cette activité, si cela s'avérait nécessaire.

Nouveau projet, nouveau départ

Mettons qu'un nouveau projet nécessitant l'utilisation de Windows débute ; voici ce qui se passe :

1. l'image de disque propre est clonée, pour donner naissance à une nouvelle image de disque, en tout point identique ; c'est la *décongélation* ;
2. la nouvelle image de disque, issue de la décongélation, peut maintenant être démarrée dans son compartiment étanche ; elle servira **exclusivement** pour le nouveau projet, et devient désormais une image *sale* ;
3. au sein de cette nouvelle image *sale*, un nouvel utilisateur Windows est créé ; le nom qui lui est attribué doit être différent **à chaque fois** qu'un nouveau projet est ainsi démarré, et cet utilisateur servira **exclusivement** pour ce nouveau projet. Ceci, parce que les logiciels tendent à inscrire le nom de l'utilisateur actif dans les métadonnées des fichiers qu'ils enregistrent, et qu'il vaut mieux éviter de rendre possibles de fâcheux recoupements.

page 21

La recette créer une nouvelle machine virtuelle à partir d'une image propre explique les détails techniques de la chose.

page 162

Maintenant que nous avons un compartiment étanche, voyons comment y ouvrir des portes sélectivement, en fonction des besoins.

Comment envoyer des fichiers au Windows embastillé ? Vu que le Windows *invité* n'a pas le droit de sortir de sa boîte pour aller chercher lui-même des fichiers, il peut être nécessaire de lui en faire parvenir depuis « l'extérieur », par exemple :

- de la matière première (*rushes*, images ou textes provenant d'autres sources) ;
- un logiciel nécessaire au nouveau projet, et absent de l'image virtuelle *décongelée*.

Nous avons déjà vu comment procéder, mais c'était dans un cas très particulier : l'installation de nouveaux logiciels dans un Windows « propre » *invité*. Partager des fichiers avec un Windows « sale » requiert davantage de réflexion et de précautions, que nous allons maintenant étudier.

La façon de faire est légèrement différente, en fonction du support sur lequel se trouvent, à l'origine, les fichiers à importer (CD, DVD, clé USB, dossier présent sur le disque dur du système chiffré), mais les précautions d'usage sont les mêmes :

- Windows doit **uniquement** avoir accès aux fichiers qu'on veut y importer, et c'est tout. Il n'est pas question de lui donner accès à un dossier qui contient, pêle-mêle, des fichiers concernant des projets qui ne devraient pas être recoupés entre eux. Si ça implique de commencer par une phase de tri et de rangement, et bien, soit.
- Lorsque Windows a besoin de *lire* (recopier) les fichiers contenus dans un dossier, on lui donne **uniquement** accès en *lecture* à ce dossier. Le moins on donne le droit à Windows d'écrire ici ou là, le moins il laissera de traces gênantes.

À noter que, lorsqu'on décide de partager un dossier du système hôte avec un Windows *invité*, VirtualBox propose de rendre ce partage permanent. Ça évite de refaire la manipulation à chaque fois qu'il est nécessaire d'envoyer un fichier au Windows *invité*, mais ça implique le risque de déposer des fichiers dans ce dossier sans penser qu'ils pourront être lisibles par Windows et ses sbires.

C'est pourquoi, afin d'éviter de se mélanger les pinceaux, nous recommandons de :

- créer **un** dossier d'importation par projet ;
- nommer ce dossier de façon aussi explicite que possible ; par exemple : *Dossier lisible par Windows* ;
- ne jamais partager d'autres dossiers que celui-ci avec le Windows *invité*.

La recette « envoyer des fichiers au système virtualisé » explique comment procéder pratiquement.

page 164

Comment faire sortir des fichiers du Windows embastillé? Le Windows *invité* n'a pas le droit, par défaut, de laisser des traces en dehors de son compartiment étanche. Mais presque inévitablement vient le temps où il est nécessaire d'en faire sortir des fichiers, et à ce moment-là, il nous faut l'autoriser explicitement, par exemple :

- pour emmener à la boîte-à-copies, ou chez l'imprimeur, un fichier PDF exporté ;
- pour projeter, sous forme de DVD, le film fraîchement réalisé.

Lorsqu'on doit récupérer un CD ou DVD non chiffré, et que la machine hôte est munie d'un graveur, il suffit de « prêter » ce périphérique, temporairement, au Windows *invité*, afin de graver depuis ce système.

Dans le cas où rien n'oblige à récupérer les fichiers sur un support non chiffré, il est possible de les exporter vers un dossier vide, dédié à cet usage, et stocké sur un volume chiffré qui peut être :

- une clé USB chiffrée, qu'on active sous Debian en tapant la phrase de passe correspondante ;
- le disque dur de la Debian chiffrée qui fait ici office de système *hôte*.

Ce dossier dédié sera partagé, via VirtualBox, avec le Windows *invité*. Insistons sur les mots **vide** et **dédié** : Windows pourra lire et modifier tout ce que ce dossier contient, et il serait dommageable de lui permettre de lire des fichiers, quand on a seulement besoin d'exporter un fichier.

Afin d'éviter de se mélanger les pinceaux et de limiter la contagion, nous recommandons de :

- créer **un** dossier d'exportation par projet ;
- nommer ce dossier de façon aussi explicite que possible ; par exemple : *Dossier où Windows peut écrire* ;
- ne jamais partager d'autres dossiers que celui-ci avec le Windows *invité*, mis à part le dossier d'importation que le paragraphe précédent préconise.

page 166
page 137

Les recettes « récupérer des fichiers depuis un système virtualisé » et « chiffrer une clé USB » expliquent comment procéder pratiquement.

Quand le projet est terminé

Quand ce projet est terminé, il faut faire le ménage, mais avant toute chose :

1. l'œuvre résultante est exportée sur le support approprié (papier, VHS, *etc.*), en s'aidant du paragraphe précédent, qui explique comment faire sortir des fichiers du Windows *invité* ;
2. les fichiers de travail sont, si nécessaire, archivés (le cas d'usage suivant traitant, quelle coïncidence, de la question).

page 77

Puis vient l'heure du grand ménage, qui éliminera du système *hôte* le plus possible de traces du projet achevé :

- l'image de disque sale est retirée de VirtualBox et effacée « pour de vrai » ;
- le dossier d'importation est effacé « pour de vrai » ;
- le dossier d'exportation est effacé « pour de vrai »... après avoir vérifié, une dernière fois, que tout ce qui doit être conservé a bien été archivé ailleurs.

page 161
page 129

Les recettes « effacer des images de disque » et « effacer des fichiers » expliquent comment effectuer ces opérations.

Encore un nouveau projet ?

Si un nouveau projet survient, nécessitant lui aussi d'utiliser Windows, ne réutilisons **pas** le même Windows *sale*. Retournons plutôt à l'étape « nouveau projet, nouveau départ ».

page 71

9.6.3 Troisième étape : attaques possibles et contre-mesures

L'hypothèse que nous venons de décrire est basée sur l'utilisation, comme système *hôte*, de la Debian chiffrée mise en place à la première étape du cas d'usage « un nouveau départ ». Toutes les attaques concernant cette Debian chiffrée sont donc applicables à la présente solution. Il est donc maintenant temps d'étudier les attaques praticables contre ce système.

page 58

Traces laissées sur notre Debian chiffrée

La **plupart** des traces **les plus évidentes** de ce projet sont séparées du reste du système : tous les fichiers de travail sont stockés dans le fichier contenant l'image de disque virtuel. Le nom de la machine virtuelle, sa configuration ainsi que ses périodes d'utilisation laisseront par contre d'autres traces sur notre système Debian.

Si la catastrophe arrive pendant la réalisation du projet Le disque dur de l'ordinateur utilisé contient les fichiers de travail à l'intérieur de l'image de disque virtuel.

Si la catastrophe arrive plus tard L'image de disque virtuel étant convenablement nettoyée lorsque le projet est achevé, **si** la catastrophe (céder face à la loi, découverte d'un problème dans le système cryptographique) arrive **après coup**, les traces résiduelles sur le disque dur seront moins évidentes, et moins nombreuses, que si l'on avait procédé de façon ordinaire.

Même si la catastrophe arrive après la fin du projet, c'est-à-dire : après le nettoyage conseillé ici, il serait malvenu de se sentir immunisé, car comme le début de ce cas d'usage l'explique, l'inconvénient majeur de la méthode décrite ici est qu'elle est basée sur le principe de liste noire, principe abondamment décrié en ces pages... et il restera donc toujours des traces indésirables, auxquelles on n'avait pas pensé, sur le disque dur de l'ordinateur utilisé, en plus de celles qu'on connaît bien désormais : journaux, mémoires vive et « virtuelle », sauvegardes automatiques.

page 65

page 53

page 19

Si, malgré ces soucis, l'hypothèse que nous venons de décrire semble être un compromis acceptable, il est maintenant nécessaire de se renseigner sur les limites partagées par toutes les solutions envisagées dans ce cas d'usage.

page 75

Sinon, creusons un peu.

Aller plus loin

Admettons qu'une des attaques décrites à partir de la troisième étape du cas d'usage « un nouveau départ » semble crédible. Si elle réussissait, le contenu du disque dur chiffré du système *hôte* serait lisible, en clair, par l'attaquant. Or nos fichiers de travail sont, rappelons-le, contenus dans l'image de disque virtuel utilisée par notre Windows *invité*... qui est un bête fichier stocké sur le disque dur du système *hôte*. Ces fichiers de travail, ainsi que toute trace enregistrée par les logiciels utilisés dans Windows, deviennent alors lisibles par l'attaquant.

page 59

Nous allons envisager deux pistes permettant de limiter les dégâts. L'une est de type « liste noire », l'autre est de type « liste blanche ».

Stocker l'image de disque virtuel en dehors du disque du système *hôte*

Une idée est de stocker hors du disque dur du système *hôte* l'image de disque virtuel utilisée par le système Windows *invité*. Par exemple, sur un disque dur externe chiffré. Ainsi, même si le disque du système *hôte* est déchiffré, nos fichiers de travail restent inaccessibles... pourvu que le disque dur externe qui les contient soit, à ce moment-là, convenablement « rangé ».

[page 53] Cette approche est de type « liste noire », avec tous les problèmes que ça pose. Les fichiers de travail et le système Windows sont certes extraits du disque dur du système *hôte*, mais il ne faut pas oublier une chose : ces données seront utilisées par un logiciel animé par le système *hôte*, nommément : VirtualBox. Comme le chapitre « traces à tous les étages » l'explique, diverses traces subsisteront donc, inévitablement, sur le disque dur **interne** de l'ordinateur utilisé.

Pour suivre cette piste :

- [page suivante] • se renseigner sur les limites partagées par toutes les solutions envisagées dans ce cas d'usage ;
- [page 137] • se reporter à la recette permettant de chiffrer un disque dur externe.

Utiliser un système *live* comme système *hôte* Le pendant de cette approche « liste noire » est une solution de type « liste blanche », conjuguant l'utilisation d'un système *live*, et le stockage de l'image de disque virtuel sur un disque dur externe chiffré.

Pour suivre cette piste :

- [page suivante] • se renseigner sur les limites partagées par toutes les solutions envisagées dans ce cas d'usage ;
- [page 137] • se reporter à la recette permettant de chiffrer un disque dur externe, et à celle qui explique comment utiliser un système *live*.
- [page 99]

9.7 Nettoyer les métadonnées du document terminé

Une fois notre document terminé, on l’exportera dans un format adapté à l’échange de documents – par exemple un PDF pour imprimer un texte, un fichier AVI ou Ogg pour publier une vidéo sur Internet, *etc.*

Considérons qu’on publie notre document sans prendre de plus amples précautions : un adversaire à qui il déplairait va probablement tout simplement commencer par télécharger le document en quête d’éventuelles métadonnées qui le rapprocheraient de ses auteurs.

Malgré les précautions qu’on a déjà prises, il est bon de nettoyer les éventuelles métadonnées présentes. [page 175]

9.8 Limites communes à ces politiques de sécurité

Toute politique de sécurité étudiée dans ce cas d’usage est vulnérable à un certain nombre d’attaques. Ce, qu’elle soit basée sur un système *live* ou sur l’envoûtement de l’infâme Windows.

Les étapes 4 et 5 du nouveau départ étudient certaines des attaques imaginables, relevant plus ou moins de la science-fiction, selon l’époque, le lieu, les protagonistes et les circonstances. Le moment est venu de les relire d’un œil nouveau. [page 57]

Par ailleurs, la partie « problématiques » de ce tome abordait, de façon relativement générale, de nombreux modes de surveillance, qu’il peut être bon de réétudier à la lumière de la situation concrète qui nous occupe ; nommons en particulier les questions d’électricité, champs magnétiques et ondes radios, ainsi que les effets des divers mouchards. [page 7]
[page 14]
[page 23]

Cas d'usage : archiver un projet achevé

10.1 Contexte

Un projet sensible touche à sa fin ; par exemple, un livre a été maqueté et imprimé, un film a été monté, compressé, et gravé sur DVD.

[page 65]

En général, il ne sera dès lors plus nécessaire de pouvoir accéder en permanence aux fichiers de travail (iconographie en haute résolution, *rushes* non compressés). Par contre, il peut être utile de pouvoir les retrouver plus tard, par exemple pour une réédition, une version mise à jour...

Vu qu'un système est d'autant plus susceptible d'être *attaqué* qu'il est fréquemment utilisé, autant extraire les informations rarement utilisées de l'ordinateur utilisé quotidiennement. De surcroît, il est plus facile de nier tout lien avec des fichiers, lorsqu'ils sont stockés sur une clé USB au fond d'un bois, que lorsqu'ils sont rangés sur le disque dur de l'ordinateur familial.

10.2 Est-ce bien nécessaire ?

La première question à se poser avant d'archiver de tels fichiers est la suivante : est-il *vraiment* nécessaire de les conserver ? Lorsqu'on ne dispose plus *du tout* d'une information, quiconque aura beau insister, personne ne sera en mesure de la donner, et c'est parfois la meilleure solution.

10.3 Évaluer les risques

10.3.1 Que veut-on protéger ?

Que donnent les catégories définies lorsque nous parlons d'évaluation des risques, appliquées à ce cas ?

[page 49]

- confidentialité : éviter qu'un œil indésirable ne tombe trop aisément sur les informations archivées ;
- intégrité : éviter que ces informations ne soient modifiées à notre insu ;
- accessibilité : faire en sorte que ces informations restent accessibles quand on en a besoin.

Ici, l'accessibilité est secondaire par rapport à la confidentialité : toute l'idée de l'archivage est de faire un compromis, en rendant l'accès aux données plus difficile *pour tout le monde*, afin de leur offrir une meilleure confidentialité.

10.3.2 Contre qui veut-on se protéger ?

Les risques envisagés dans notre « nouveau départ » sont valables ici aussi : un

[page 57]

cambrilage, une perquisition ayant des motifs qui ne sont pas directement liés aux informations qu'on veut ici protéger.

Ajoutons, à ces risques, la possibilité que le livre ou le film produit déplaie à quelque commissaire, ministre, P.D.G. ou assimilé. Ça arrive. Admettons que :

- cette autorité a eu vent d'indices lui permettant de soupçonner qui a commis le chef d'œuvre ;
- cette autorité est en mesure de mandater une cohorte de pénibles hommes en armes et uniforme, au petit matin et au domicile des personnes soupçonnées.

Une telle inopportune intrusion débouchera au minimum, de façon tout aussi fâcheuse qu'évidente, sur la saisie de tout matériel informatique qui pourra y être découvert. Ce matériel sera ensuite remis, par les intrus, à un autre homme de main des autorités, qui pratiquera un genre d'autopsie visant à mettre au jour les données stockées sur ce matériel... ou l'ayant été.

page 32

10.4 Méthode

La méthode la plus simple à l'heure actuelle est :

page 137

1. créer une clé USB ou un disque dur externe chiffré ;

2. copier les fichiers à archiver vers ce périphérique ;

page 127

3. supprimer et écraser le contenu des fichiers de travail.

Une fois ces opérations effectuées, la clé ou le disque dur pourra être entreposé dans un autre lieu que l'ordinateur utilisé couramment.

On pourrait envisager l'utilisation de CD ou de DVD, pour leur faible coût, mais à l'heure actuelle, il est plus complexe de chiffrer correctement des données sur ces supports que sur des clés USB, qui sont désormais monnaie courante et faciles à se procurer.

10.5 Quelle phrase de passe ?

page 91

Vu que les fichiers seront archivés sous forme chiffrée, il sera nécessaire de choisir une phrase de passe. Or, vu que la vocation est l'archivage, cette phrase de passe ne sera pas souvent utilisée. Et une phrase de passe rarement utilisée a toutes les chances d'être oubliée... rendant impossible l'accès aux données.

Face à ce problème, on peut envisager quelques pistes.

10.5.1 Écrire la phrase de passe quelque part

Toute la difficulté étant de savoir où l'écrire, ranger ce document pour pouvoir le retrouver... sans pour autant que d'autres puissent le retrouver et l'identifier comme une phrase de passe.

10.5.2 Utiliser la même phrase de passe que pour son système quotidien

page 105

La phrase de passe de son système quotidien, dans le cas où il est chiffré, est une phrase qu'on tape régulièrement, et dont on a toutes les chances de se souvenir.

Par contre :

- si on est forcé de révéler la phrase de passe commune, l'accès à l'archive devient également possible ;

- il est nécessaire d'avoir **très fortement** confiance dans les ordinateurs avec lequel on accèdera aux archives. Sinon, on peut se faire « piquer », à son insu, la phrase de passe, qui pourra ensuite être utilisée pour lire non seulement les informations archivées, mais aussi toutes les données stockées sur l'ordinateur.

10.5.3 Partager le secret à plusieurs

Il est possible de partager un secret à plusieurs. Cela impose de réunir plusieurs personnes afin de pouvoir accéder au contenu archivé. C'est à peser : ça peut compliquer la tâche aussi bien pour des accès désirés qu'indésirables.

page 149

10.6 Un disque dur ? Une clé ? Plusieurs clés ?

Selon les choix faits précédemment, entre autres sur la phrase de passe, on peut se demander quels supports utiliser. Sachant que sur le plan technique, le plus simple actuellement est d'avoir une seule phrase de passe par support.

Un disque dur externe peut contenir plus de données qu'une clé USB, et est donc parfois nécessaire : pour archiver un projet de vidéo, par exemple.

Archiver plusieurs projets sur un même support permet de se simplifier la tâche, mais il devient alors difficile de séparer les projets selon les niveaux de confidentialité souhaités. Qui plus est, en procédant ainsi, les personnes pouvant accéder aux archives d'un projet ont aussi accès aux autres, ce qui n'est pas forcément souhaitable.

Par ailleurs, si la phrase de passe est un secret partagé, autant faciliter l'accès aux personnes partageant le secret, en ayant un support qu'elles peuvent se transmettre.

01 001
100 0010
01
0000111
11100000 0000
00100010 1111
00011 00

00 0010
0000 0011 111
101 01010
1010001 111
000111011 100
10111010 0000
00001 11

0110 0010
10010 1011
011 0011
101010011 1101
101110011
101101 1110
0111 001

001
010 011
101 11 1011
000 100
00011 00
111001111 10100
110001111 111
00000101 100 1011
001 0100 1101 0010
110 0000
001 000100110 0011
1000000 0011 001110100 100
101 10 1010 011001
00 010
0000001
100000111 01010
110011000 1000
001110

10
000 1111
0111 100 000
000 01010
011011100
010001011 0011
0110000 1010
0010

1011 1001
1110 0011
0011 01001
01101100 010
101010001 1111
0010001 0010
1000 10

10
1100
111 010 1110
0111 1100
01010
01100011 0000
11000010 0101
01110110 00
0011

0011 1000
0010 1100
01111
01001100 010
111010000 10
1111110 0011
1100 00

TROISIÈME PARTIE

Outils

Dans cette troisième partie, nous expliquerons comment appliquer concrètement quelques-unes des pistes évoquées précédemment.

Cette partie n'est qu'une annexe technique aux précédentes : une fois comprises les problématiques liées à l'intimité dans le monde numérique ; une fois les réponses adaptées choisies, reste la question du « Comment faire ? », à laquelle cette annexe apporte certaines réponses.

Du bon usage des recettes

Les outils et recettes qui suivent sont des solutions extrêmement partielles, qui ne sont d'aucune utilité tant qu'elles ne font pas partie d'un ensemble de pratiques articulées de façon cohérente.

Piocher dans cette boîte à outils sans avoir, au préalable, étudié la partie sur le choix d'une réponse adaptée et défini une *politique de sécurité*, est un moyen remarquable de se tirer une balle dans le pied en croyant, à tort, avoir résolu tel ou tel problème.

[page 47]

On ne peut pas faire plaisir à tout le monde

Partons du principe, pour la plupart des recettes présentées dans ce guide, que l'on utilise GNU/Linux avec le bureau GNOME ; elles ont été écrites et testées sous Debian GNU/Linux version 6.0 (surnommée Squeeze)¹ et Tails² (*The Amnesic Incognito Live System*).

Pour autant, ces recettes sont généralement concoctables avec d'autres distributions basées sur Debian, telles qu'Ubuntu³ ou gNewSense⁴.

Si l'on n'utilise pas encore GNU/Linux, ou pourra consulter le cas d'usage un nouveau départ ou utiliser un système live.

[page 57]

[page 99]

-
1. <http://www.debian.org/releases/squeeze/>
 2. <https://tails.boum.org/>
 3. <http://www.ubuntu-fr.org/>
 4. <http://www.gnewsense.org/Main.fr/HomePage>

De la bonne interprétation des recettes

Avant de passer aux recettes elles-mêmes, quelques remarques transversales nous ont paru nécessaires.

Dans un certain nombre d'outils, les procédures sont présentées pas à pas, et expliquent, chaque fois que c'est possible, le sens des actions que l'on propose d'effectuer. Une utilisation efficace de ces outils nécessite de s'entendre sur quelques points :

- L'ordre dans lequel chaque recette est développée est d'une importance capitale. Sauf mention contraire, il est simplement inimaginable de sauter une étape pour ensuite revenir en arrière : le résultat, si jamais ces opérations désordonnées en donnaient un, pourrait être soit différent de celui escompté, soit tout bonnement catastrophique.
- Dans le même ordre d'idée, les actions indiquées doivent être effectuées à la lettre. Omettre une option, ouvrir le mauvais dossier, peut avoir pour effet de totalement modifier le sens ou les effets d'une recette.
- De manière générale, la bonne compréhension de ces recettes demande d'y accorder un minimum d'attention et de vivacité d'esprit. On ne peut pas tout réexpliquer à chaque fois : il est implicite d'avoir auparavant « suivi » et intégré les explications des « cas d'usage » dont ces recettes ne sont que la dernière étape.

Enfin l'exemplaire que vous avez entre les mains n'est pas forcément à jour aux vues des versions actuelles des différents outils impliqués. La version en ligne [<https://guide.boum.org/>] du Guide d'Autodéfense Numérique a des chances d'être plus à jour.

Utiliser un terminal

🔄 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

🕒 *Durée : 15 à 30 minutes.*

Souvent, on utilise un ordinateur personnel en cliquant sur des menus et des icônes. Cependant, il existe une autre façon de lui « parler » : en tapant des bouts de texte que l'on appelle des « commandes ». On appelle cette façon d'interagir avec un ordinateur « le terminal », « le *shell* » ou encore « la ligne de commande ».

Ce guide cherche le plus souvent possible à contourner l'utilisation de cet outil, qui est assez déroutant lorsque l'on n'y est pas habitué. Cependant, son usage s'est parfois avéré indispensable.

11.1 Qu'est-ce qu'un terminal ?

Une explication détaillée sur l'usage de lignes de commandes n'est pas l'objet de ce guide, et Internet regorge de tutoriels et de cours assurant très bien ce rôle¹. Il semblait cependant nécessaire de poser quelques bases sur la manière de s'en servir.

Alors on va tout simplement commencer par ouvrir un terminal : sur un bureau GNOME standard, il suffit de cliquer sur *Applications* → *Accessoires* → *Terminal*. Apparaît alors une fenêtre qui indique :

```
IDENTIFIANT@LE_NOM_DE_LA_MACHINE :~$
```

À la fin se trouve un carré, appelé « curseur », qui correspond à l'endroit où inscrire le texte de la commande. Concrètement, avec l'identifiant *roger* sur une machine nommée *debian*, on aura sous les yeux :

```
roger@debian :~$ █
```

C'est à partir de cet état, appelé « invite de commande », que l'on peut taper directement les commandes qu'on veut faire exécuter à l'ordinateur.

L'effet final de ces commandes est souvent le même que celui qu'on peut obtenir en cliquant au bon endroit dans une interface graphique.

¹. Entre autres, une [page sur ubuntu-fr.org](http://doc.ubuntu-fr.org/console) [<http://doc.ubuntu-fr.org/console>] qui se termine elle-même par d'autres liens.

Par exemple, si dans le terminal qu'on vient d'ouvrir, on écrit juste `gedit` puis qu'on tape sur *Entrée*, le résultat est qu'on ouvre un éditeur de texte. On aurait pu faire exactement la même chose en cliquant sur *Applications* → *Accessoires* → *Éditeur de texte gedit*. Par contre, on ne pourra pas entrer de nouvelle commande dans notre terminal tant que l'on aura pas quitté l'éditeur de texte.

Dans le cadre de ce guide, l'intérêt du terminal est surtout qu'il permet d'effectuer des actions qu'aucune interface graphique ne propose pour le moment.

11.2 À propos des commandes

Les commandes sont comme des ordres qu'on donne à l'ordinateur par le biais du terminal. Ces « lignes de commande » ont leur propre langage, avec leurs mots, leurs lettres, et leur syntaxe. Quelques remarques à ce sujet sont donc utiles.

11.2.1 Syntaxe

Prenons par exemple cette commande, `sfill`, qui permet à peu près les mêmes opérations que `nautilus-wipe`, un outil graphique qui sera présenté plus tard :

page 135

<u>sfill</u>	<u>-l</u>	<u>-v</u>	<u>/home</u>
commande	option	option	argument

Dans cette ligne de commande, on peut voir, dans l'ordre :

- la *commande* que l'on appelle est `sfill`. La commande est en général un programme installé sur le système ;
- deux *options*, `-l` et `-v` qui modifient le comportement du programme `sfill`. Ces dernières peuvent être facultatives selon le programme (et commencent par un ou deux tiret pour qu'on les distingue) ;
- un *argument* `/home` qui précise ce sur quoi va travailler la commande. Il peut y en avoir plusieurs, ou aucun, tout dépend de la commande.

Chacun de ces éléments doit être séparé des autres par un (ou plusieurs) espace(s). Il y a donc un espace entre la commande et la première option, entre la première option et la suivante, entre la dernière option et le premier argument, entre le premier argument et les suivants, *etc.*

Pour savoir quelles sont les commandes disponibles, leurs options et leurs arguments, pas de mystère : chaque commande dispose normalement d'une page de manuel. Pour y accéder, il suffit d'aller dans *Système* → *Aide*, puis dans *Pages de manuel*. Ces dernières peuvent toutefois être difficiles à comprendre par leur aspect technique, et ne sont parfois disponibles qu'en anglais.

11.2.2 Insertion du chemin d'un fichier

Lors de l'utilisation d'un terminal, on a souvent besoin d'indiquer des dossiers et des fichiers. On parle de « chemin » car on décrit généralement dans quel dossier et sous-dossier un fichier se trouve. Pour séparer un dossier de ce qu'il contient, on utilise le caractère `/` (qui se prononce « slash »).

Pour donner un exemple, voici le *chemin* du document `recette.txt` qui se trouve dans le dossier `Documents` du dossier personnel du compte `alligator` :

```
/home/alligator/Documents/recette.txt
```


Comme beaucoup de commandes attendent des noms de fichiers comme arguments, cela devient vite fastidieux de taper leurs chemins complets à la main. Il y a cependant un moyen simple d'insérer un chemin : quand on attrape avec la souris l'icône d'un fichier, et qu'on le déplace pour le lâcher sur le terminal, son chemin s'écrit là où se trouve le curseur.

Cela ne marche cependant qu'avec les vrais fichiers ou dossiers. On obtiendra un nom bizarre qui ne fonctionnera pas, par exemple, pour les fichiers mis à la corbeille, l'icône du *Dossier personnel* sur le bureau ou avec les icônes de clés USB.

11.2.3 Exécution

Une fois que l'on a tapé une commande, on demande à l'ordinateur de l'« exécuter » en appuyant sur la touche *Entrée*.

11.2.4 Fin ou interruption de la commande

L'exécution de la commande prend plus ou moins de temps. Lorsqu'elle est terminée, le terminal retourne toujours à l'état où il était avant qu'on lance la commande, l'« invite de commande » :

```
roger@debian :~$ █
```

On dit alors que le terminal « rend la main ».



Si on souhaite interrompre l'exécution d'une commande avant qu'elle soit terminée, on peut appuyer la touche **Ctrl**, et tout en laissant cette touche enfoncée appuyer sur la touche **C**. On arrête alors la commande immédiatement, un peu comme quand on ferme la fenêtre d'un programme.

11.2.5 Typographie

La plupart des symboles utilisés pour entrer les commandes complètes sont des symboles courants. Lorsqu'une commande emploie le symbole « - », il ne s'agit que du « tiret » qu'on peut obtenir en tapant (sur un clavier français) la touche **6**. Pour un « ' » (apostrophe droite), c'est le **4** ...

D'autres symboles sont rarement utilisés en dehors du terminal, mais sont disponibles avec les claviers standards. Ils sont mêmes indiqués sur le clavier, et accessibles à l'aide de la touche **Alt** de droite, notée **AltGr**. Voici, en se basant sur un clavier de PC français standard, la correspondance de quelques touches avec les symboles qu'elles écrivent, et leur nom (bien peu seront en fait utilisées dans ce guide) :

Touches	Résultat	Nom du symbole
AltGr + 2	~	tilde
AltGr + 3	#	dièse
AltGr + 4	{	accolade gauche
AltGr + 5	[crochet gauche
AltGr + 6		<i>pipe</i>
AltGr + 8	\	antislash
AltGr + 0	@	arobase
AltGr +]]	crochet droit

Touches	Résultat	Nom du symbole
 + 	}	accolade droite

11.2.6 Noms à remplacer

Parfois, on précise que l'on va nommer quelque chose que l'on a trouvé pour le réutiliser plus tard. Par exemple, on dira que l'identifiant est `LOGIN`. Mettons qu'on travaille sous l'identifiant `paquerette`. Lorsqu'on écrira « taper `LOGIN` en remplaçant `LOGIN` par l'identifiant de son compte », il faudra taper en réalité `paquerette`. Si l'on tape `LOGIN`, cela ne fonctionnera pas...

11.3 Terminal? Terminal administrateur?

Dans le menu *Applications* → *Accessoires* se trouvent deux entrées permettant d'obtenir un terminal : *Terminal* et *Terminal administrateur*.

La première permet d'obtenir un terminal fonctionnant avec les droits d'accès de la session en cours. On ne pourra donc pas l'utiliser pour effectuer des opérations *privilegiées* comme créer une partition chiffrée. Le symbole à la fin de l'« invite de commande » sera un dollar (\$).

La seconde commande permet d'obtenir un terminal avec les droits d'administration. On appelle également cela un *shell root*. À partir de ce dernier, les commandes pourront accéder à l'intégralité du système, sans restriction... avec les risques que cela comporte, donc. Le symbole à la fin de l'« invite de commande » sera un dièse (#).

11.4 Encore une mise en garde

Plus encore que pour les recettes dont on parlait plus haut, les commandes doivent être tapées très précisément. Oublier un espace, omettre une option, se tromper de symbole, être imprécis dans un argument, c'est changer le sens de la commande.

Et comme l'ordinateur effectue *exactement* ce qui est demandé, si on change la commande, il fera *exactement autre chose*...

11.5 Un exercice

On va créer un fichier vide nommé « `essai` », qu'on va ensuite supprimer (sans recouvrir son contenu).

Dans un terminal, entrer la commande :

```
$> touch essai
```

Et taper sur *Entrée* pour que l'ordinateur l'exécute.

La *commande* `touch` donne l'ordre de créer un fichier vide ; l'*argument* `essai` donne le nom de ce fichier. Aucune option n'est utilisée.

On peut alors vérifier que ce fichier a été créé en lançant la commande `ls` (qui signifie « lister ») :

```
$> ls
```

Une fois la commande lancée, l'ordinateur répond avec une liste. Sur celui utilisé pour les tests, cela donne :

```
Bureau
essai
```

Bureau est le nom d'un dossier qui existait déjà avant, et **essai** le nom du fichier qu'on vient de créer. Un autre ordinateur auraient pu répondre avec de nombreux autres fichiers en plus de Bureau et de **essai**.

Ce que répond la commande `ls` n'est qu'une autre manière de voir ce que l'on peut obtenir par ailleurs. En cliquant, sur le bureau, sur l'icône du *Dossier personnel*, on pourra noter dans le navigateur de fichiers l'apparition d'une nouvelle icône représentant le fichier **essai** que l'on vient juste de créer...

On va maintenant supprimer ce fichier. La ligne de commande pour le faire a pour syntaxe générale :

```
rm [options] NOM_DU_FICHIER_A_SUPPRIMER
```

On va utiliser l'option `-v` qui, dans le cadre de *cette* commande, demande à l'ordinateur d'être « bavard » (on parle de « mode verbeux ») sur les actions qu'il va effectuer.

Pour insérer le nom du fichier à supprimer, on va utiliser l'astuce donnée précédemment pour indiquer le chemin du fichier. On va donc :

- taper `rm -v` dans notre terminal,
- taper un espace afin de séparer l'option `-v` de la suite,
- dans la fenêtre du *Dossier personnel*, on va prendre avec la souris l'icône du fichier **essai** et la déposer dans le terminal.

À la fin de cette opération, on doit obtenir quelque chose comme :

```
$>
```

```
rm -v '/home/LOGIN/essai'
```

On peut alors appuyer sur la touche *Entrée* et constater que l'ordinateur répond :

```
« /home/LOGIN/essai » supprimé
```

Cela indique qu'il a bien supprimé le fichier demandé. On peut encore vérifier son absence en lançant un nouveau `ls` :

```
$>
```

```
ls
```

On doit constater l'absence de **essai** dans la liste que nous répond la commande. Sur le même ordinateur que tout à l'heure, cela donne :

```
Bureau
```

Et l'icône doit également avoir disparu dans le navigateur de fichiers. Apparemment, il a été supprimé... même si, comme expliqué dans la première partie, son contenu existe encore sur le disque. Comme c'était un fichier vide nommé « **essai** », on peut se dire que ce n'est pas bien grave.

11.6 Attention aux traces !

page 21 La plupart des *shells* enregistrent automatiquement les lignes de commande que l'on a tapées dans un fichier « d'historique ». C'est bien pratique pour retrouver plus tard des commandes que l'on a pu utiliser, mais cela laisse également sur le disque une trace de nos activités.

Le *shell* standard dans Debian s'appelle `bash`. Avec ce dernier, pour désactiver temporairement l'enregistrement de l'historique dans le terminal que l'on utilise, il suffit de faire :



```
unset HISTFILE
```

page 129 Par ailleurs, les commandes sont enregistrées dans le fichier caché `.bash_history` (qui se trouve dans le *Dossier personnel*). On peut donc avoir envie de le nettoyer de temps en temps.

11.7 Pour aller plus loin

Cette première expérience avec cette fenêtre pleine de petits caractères pourrait être le début d'une longue passion. Pour l'entretenir, rien de mieux que de prendre le temps de lire le chapitre « Débuter en console² » de la *formation Debian* ou celui baptisé « Linux en mode texte : consolez-vous!³ » du livre *Linux aux petits oignons*.

2. <http://formation-debian.via.ecp.fr/debuter-console.html>

3. http://www.editions-eyrolles.com/Chapitres/9782212124248/Pages-63-82_Novak.pdf

Choisir une phrase de passe

🔄 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

🕒 *Durée : 10 minutes environ.*

Une « phrase de passe » (ou *passphrase* en anglais) est un secret qui sert à protéger des données chiffrées. C'est ce qu'on utilise pour chiffrer un disque dur, des emails, des documents... voire comme nous le verrons dans le second tome de cet ouvrage, des clés cryptographiques.

On parle de *phrase* plutôt que de *mot* de passe car un seul *mot*, aussi bizarre et compliqué soit-il, est beaucoup moins résistant qu'une simple phrase de plusieurs mots. On considère qu'une phrase de passe doit être constituée d'au moins 10 mots. Mais plus il y en a, mieux c'est !

Un critère important, mais parfois négligé : une bonne phrase de passe est une phrase de passe dont on peut *se souvenir*¹, ça évite de la noter sur un papier, grave erreur qui rend caduc l'intérêt de se faire une phrase de passe béton. Mais, et c'est tout aussi important, une bonne phrase de passe doit être *impossible à deviner*. Évitions donc les phrases de passe formées de 15 mots composés de caractères aléatoires qu'on aura oublié à peine 15 minutes après l'avoir trouvé.

Une technique simple pour trouver une bonne phrase de passe, difficile à deviner, mais néanmoins facile à retenir, est de fabriquer une phrase qui n'est pas issue d'un texte existant. En effet, que ce soit des paroles de chansons, le vers d'un poème, ou une citation d'un livre, des outils comme le projet Gutenberg² rendent de plus en plus facile le test de phrases de passe tirées de la littérature existante³.

Même s'il faut ici vous en remettre à votre imagination, nous pouvons quand même donner quelques pistes quant aux bonnes habitudes à avoir lors du choix d'une phrase de passe.

1. Fabriquons tout d'abord une phrase dont on se souviendra aisément. Faisons tourner nos méninges un instant.
2. Trouvons dans cette phrase ce que l'on peut modifier pour la rendre plus difficilement devinable. On peut ainsi penser à y ajouter de l'argot, des mots de

1. Randall Munroe, 2014, *Password Strength* [<https://xkcd.com/936/>] (en anglais).
2. Wikipédia, 2014, *Projet Gutenberg* [https://fr.wikipedia.org/wiki/Projet_Gutenberg].
3. Dan Goodin, 2013, *How the Bible and YouTube are fueling the next frontier of password cracking* [<http://arstechnica.com/security/2013/10/how-the-bible-and-youtube-are-fueling-the-next-frontier-of-password-cracking/>] (en anglais).

différentes langues, mettre des majuscules là où l'on ne les attend pas remplacer des caractères par d'autres, laisser libre cours à son imagination quant à l'orthographe *etc.*

Un conseil toutefois : il est préférable d'éviter les caractères accentués ou tout autre symbole n'étant pas directement disponible sur un clavier américain. Cela peut éviter des problèmes de touches absentes ou difficiles à retrouver, et surtout de mauvais codage des caractères, si l'on est amené à taper notre phrase de passe sur un clavier différent de celui dont on a l'habitude.

Un exemple, prenons cette phrase sans sens apparent :

correct cheval pile agraphe

On peut les transformer ainsi, pour obtenir une meilleure phrase de passe :

korect sheVall-peEla! graFF

Une fois vos données chiffrées avec votre nouvelle phrase de passe, c'est une bonne idée de l'utiliser tout de suite une bonne dizaine de fois pour déchiffrer vos données. Cela permettra d'apprendre un peu à vos doigts comment la taper et ainsi de la mémoriser à la fois mentalement et physiquement.

N'oublions toutefois pas que si trouver une telle phrase de passe n'est pas sans effort, cela ne dispense aucunement d'en trouver une différente par support que l'on chiffre. L'usage d'une même phrase de passe, ou pire d'un même mot de passe, pour une variété de choses différentes, boîtes mail, compte *PayPal*, banque en ligne *etc.* peut rapidement s'avérer désastreux si elle est dévoilée.

Démarrer sur un CD, un DVD ou une clé USB

C *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

⌚ *Durée : 1 minute à 20 minutes environ.*

On va voir ici comment démarrer un ordinateur PC sur un média externe, par exemple un CD d'installation de Debian, ou un système *live* sur une clé USB ou même une carte SD.

Parfois, en particulier sur les ordinateurs modernes, c'est très simple. D'autres fois, c'est un peu à s'arracher les cheveux...

Cela se joue au tout début du démarrage de l'ordinateur, dans le micrologiciel. On a vu que c'est lui qui permet de choisir le périphérique (disque dur, clé USB, CD-ROM ou DVD, *etc.*) où se trouve le système qu'on veut utiliser. page 13

13.1 Essayer naïvement

Commencer par mettre le CD ou le DVD dans le lecteur, ou par brancher la clé, puis (re)démarrer l'ordinateur. Parfois, ça marche tout seul. Si c'est le cas, c'est gagné, lire la suite est inutile!


13.2 Tenter de choisir le périphérique de démarrage

Sur les micrologiciels récents, il est souvent possible de choisir un périphérique de démarrage au cas par cas.

(Re)démarrer l'ordinateur en regardant attentivement les tout premiers messages qui s'affichent à l'écran. Chercher des messages en anglais qui ressembleraient à :

- Press [KEY] to select temporary boot device
- [KEY] = Boot menu
- [KEY] to enter MultiBoot Selection Menu

Ces messages disent d'utiliser la touche KEY pour choisir un périphérique de démarrage. Cette touche est souvent F12 ou F10.

Sur les Mac, il existe un équivalent de cette possibilité : immédiatement après l'allumage de l'ordinateur, il faut appuyer et maintenir la touche  (parfois également

marquée `[option]`). Au bout d'un moment, on doit normalement voir apparaître le *Gestionnaire de démarrage*¹.

Mais revenons à nos PC. Souvent, le micrologiciel va trop vite, on n'a pas le temps de lire le message, de le comprendre et d'appuyer sur la touche. Qu'à cela ne tienne, une fois la bonne touche identifiée, redémarrer encore la machine et appuyer sur la touche en question (ne pas maintenir la touche enfoncée, mais la presser puis la relâcher plusieurs fois) dès l'allumage de l'ordinateur.

Avec un peu de chance, un message comme celui-ci s'affiche :

```
+-----+
| Boot Menu                               |
+-----+
|                                         |
| 1: USB HDD                             |
| 4: IDE HDD0: BDS GH87766319819        |
| 8: Legacy Floppy Drives               |
|                                         |
|   <Enter Setup>                       |
|                                         |
+-----+
```

Si ça marche, c'est gagné. Choisir la bonne entrée dans ce menu, en se déplaçant avec les flèches du clavier ↑ et ↓, puis appuyer sur *Entrée*. Par exemple, pour démarrer sur une clé USB, choisir **USB HDD**. L'ordinateur doit démarrer sur le périphérique sélectionné. Lire la suite est inutile!

13.3 Modifier les paramètres du micrologiciel

Si choisir un périphérique de démarrage temporaire ne fonctionne pas, il va falloir rentrer dans le micrologiciel pour choisir manuellement l'ordre de démarrage. Pour pimenter un peu la chose, les micrologiciels sont quasiment tous différents, de telle sorte qu'il est impossible de donner une recette qui marche systématiquement².

13.3.1 Entrer dans l'interface de configuration du micrologiciel

Encore une fois, il s'agit de (re)démarrer l'ordinateur en regardant attentivement les premiers messages qui s'affichent à l'écran. Chercher des messages en anglais qui ressembleraient à :

- Press [KEY] to enter setup
- Setup: [KEY]
- [KEY] = Setup
- Enter BIOS by pressing [KEY]
- Press [KEY] to enter BIOS setup
- Press [KEY] to access BIOS
- Press [KEY] to access system configuration
- For setup hit [KEY]

Ces messages disent d'utiliser la touche [KEY] pour entrer dans le micrologiciel. Cette touche est souvent `[Suppr]` (*Delete*, *DEL*) ou `[F2]`, parfois `[F1]`, `[F10]`, `[F12]`, `[Échap]`, `[⇧]` (*Tab*), voire autre chose encore.

1. http://support.apple.com/kb/HT1310?viewlocale=fr_FR

2. Des tutoriels illustrés pour quelques BIOS sont disponibles sur [cette page](http://www.hiren.info/pages/bios-boot-cdrom) [<http://www.hiren.info/pages/bios-boot-cdrom>]



Voici un tableau qui résume les touches d'accès au micrologiciel pour quelques fabricants d'ordinateurs communs³.

Fabricant	Modèle	Touches observées
Acer	modèles récents	F2 , Suppr
Acer	modèles anciens	Ctrl + Alt + Échap , F1
AST, ARI		Ctrl + Alt + Échap , Ctrl + Alt + Suppr
Compaq	modèles récents	F10
Compaq	modèles anciens	F1 , F2 , Suppr
CompUSA		Suppr
Cybermax		Échap
Dell	modèles récents	F2
Dell	anciens <i>desktops</i>	Ctrl + Alt + Entrée , Suppr
Dell	anciens portables	Fn + Échap , Fn + F1
eMachines		← (Tab) , Suppr , F2
Fujitsu		F2
Gateway		F1 , F2
HP		F1 , F2 , Échap
HP	tablet PC	F10 , F12
IBM	modèles récents	F1
IBM	anciens modèles	F2
IBM/Lenovo	modèles récents	F1 , F2
IBM/Lenovo	anciens modèles	Ctrl + Alt + F3 , Ctrl + Alt + Ins , Fn + F1
Intel	Tangent	Suppr
Micron		F1 , F2 , Suppr
NEC		F2
Packard Bell		F1 , F2 , Suppr
Shuttle		F1 , Suppr
Sony		F1 , F2 , F3
Tiger		Suppr
Toshiba		F1 , Échap
Toshiba	Equium	F12

Souvent, le micrologiciel va trop vite, et on n'a pas le temps de lire le message, de le comprendre et d'appuyer sur la touche. Qu'à cela ne tienne, une fois la bonne touche identifiée, redémarrer encore la machine en appuyant sur la touche en question (ne pas


3. Tim Fisher, 2014, *BIOS Setup Utility Access Keys for Popular Computer Systems* [http://pcsupport.about.com/od/fixtheproblem/a/biosaccess_pc.htm] ainsi que MichaelStevensTech, 2014, *How to access/enter Motherboard BIOS* [http://michaelstevens.tech.com/bios_manufacturer.htm] (liens en anglais).

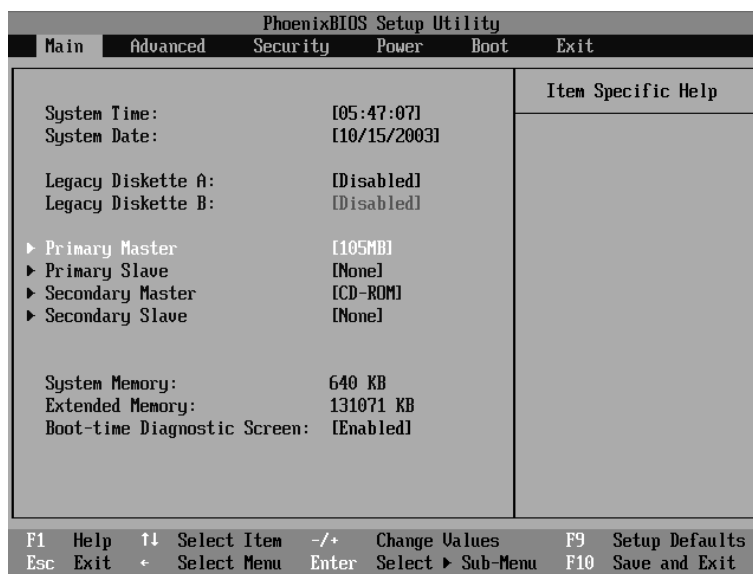
maintenir la touche enfoncée, mais la presser puis la relâcher plusieurs fois). Parfois, l'ordinateur se perd et plante. Dans ce cas, redémarrer et réessayer...

Si une image s'affiche à la place du message que l'on espère voir, il se peut que le micrologiciel soit configuré pour afficher un logo plutôt que ses messages. Essayer d'appuyer sur  ou sur  (*Tab*) pour voir les messages.

Si l'ordinateur démarre trop rapidement pour qu'on ait le temps de lire les messages qu'il affiche, il est parfois possible d'appuyer sur la touche *Pause* (souvent en haut à droite du clavier) pour geler l'écran. Réappuyer sur n'importe quelle touche peut « dégeler » l'écran.

13.3.2 Modifier la séquence de démarrage

Une fois dans le micrologiciel, l'écran est souvent bleu ou noir, et plein de menus. En général, une zone en bas ou à droite de l'écran explique comment naviguer entre les options, comment changer d'onglet... Elle est souvent en anglais : aide se dit « *help* », touche se dit « *key* », sélectionner se dit « *select* », valeur « *value* » et modifier « *modify* ». Les touches à utiliser pour se déplacer sont généralement décrites aussi, par exemple $\leftarrow \uparrow \downarrow \rightarrow$: *Move* (en anglais, déplacer se dit « *move* »). Il s'agit des flèches du clavier \downarrow et \uparrow et/ou \leftarrow et \rightarrow . Parfois, la touche  (*Tab*) est utile aussi.



Un écran de BIOS

L'idée, c'est de fouiller dedans jusqu'à trouver quelque chose qui contient *boot*, et qui ressemble par exemple à :

- First Boot Device
- Boot Order
- Boot Management
- Boot Sequence

S'il n'y a pas, tenter quelque chose comme *Advanced BIOS Features* (sur les *Award-BIOS*) ou *Advanced features* (sur les *AMIBIOS*).

Une fois la bonne entrée trouvée, il s'agit de trouver comment on la modifie. Par exemple *Enter: Select* ou *+/-: Value*. L'objectif est alors de mettre le CD/DVD ou l'USB en premier, selon sur lequel on veut démarrer.

Parfois, il faut entrer dans un sous-menu. Par exemple s'il y a un menu `Boot order` et qu'il est écrit dans l'aide `Enter: Select`, appuyer sur entrée une fois le menu sélectionné.

D'autres fois, les options se changent directement. Par exemple, s'il y a une option comme `First boot device` et qu'il est écrit dans l'aide `+/-: Value`, appuyer sur la touche `+` ou la touche `-` jusqu'à ce que la bonne valeur, comme par exemple `IDE DVDROM`, soit sélectionnée. Parfois, ce sont plutôt les touches *Page suivante* ou `PgUp` et *Page précédente* ou `PgDown` qui sont utilisées. Parfois encore, ce sont des touches comme `F5` et `F6`. D'autres fois encore, ces touches servent à monter et à descendre le périphérique dans une liste correspondant à l'ordre de démarrage.

13.3.3 Bien choisir sa nouvelle configuration

Une fois qu'on a réussi à sélectionner le bon support pour le démarrage, il faut se demander si on veut le laisser pour toujours ou pas. Si on veut le laisser, il peut être utile de placer le disque dur en deuxième position dans la séquence de démarrage. Ainsi, si le support placé en premier est absent, l'ordinateur démarrera sur le disque dur. Si l'on ne met pas le disque dur dans la séquence de démarrage, l'ordinateur ne démarrera pas dessus, même en l'absence de CD, de DVD ou de clé USB.

Cependant, le fait de laisser son ordinateur démarrer *a priori* sur un support externe peut avoir des conséquences fâcheuses : il devient un peu plus facile pour un intrus de le faire démarrer en utilisant ce support, par exemple pour effectuer une attaque.

On peut certes mettre en place, avec le micrologiciel, un mot de passe d'accès à l'ordinateur, qui devra être entré avant tout démarrage. Mais il est inutile de compter sur celui-ci pour protéger quoi que ce soit : cette protection peut, la plupart du temps, être contournée très facilement.

13.3.4 Enregistrer et quitter

Une fois la nouvelle configuration établie, il reste à enregistrer et à quitter. Encore une fois, lire l'aide à l'écran, comme `F10: Save`. Parfois, il faut appuyer une ou plusieurs fois sur `[Échap]` pour avoir le bon menu. Un message s'affiche alors pour demander (en anglais) si on est sûr de vouloir enregistrer et quitter. Par exemple :

```
+-----+
|           Setup Confirmation           |
+-----+
|                                       |
| Save configuration and exit now       |
|                                       |
|           <Yes>           <No>       |
|                                       |
+-----+
```

On veut effectivement enregistrer, donc on sélectionne `Yes` et on appuie sur *Entrée*.

Utiliser un système *live*

🔄 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

🕒 *Durée : 30 minutes à une heure, plus environ 30 minutes de téléchargement.*

Un système *live* est un système GNU/Linux qui fonctionne sans être installé sur le disque dur de l'ordinateur.

Attention, cela ne signifie pas qu'il n'y aura pas de traces sur le disque dur : par exemple, nombre de systèmes *live* utilisent l'espace d'échange (*swap*) présent sur le disque dur s'ils en détectent un. De plus, ils utilisent parfois automatiquement les partitions qu'ils y détectent.

[page 17]

14.1 Des systèmes *live* discrets

Par contre, certains systèmes *live* sont spécialement conçus pour (tenter de) ne laisser aucune trace sur le disque dur de l'ordinateur sur lequel ils sont utilisés, à moins que l'on ne leur demande expressément de le faire. C'est par exemple le cas de Tails (*The Amnesic Incognito Live System* — le système *live* amnésique incognito).

Il n'y a alors (si les personnes à l'origine du système *live* ne se sont pas trompées) rien d'écrit sur le disque dur. Tout ce qui sera fait à partir du système *live* sera uniquement écrit en mémoire vive, qui s'efface plus ou moins pour de vrai toute seule quand on éteint l'ordinateur, du moins au bout d'un certain temps.

[page 11]

Utiliser de tels systèmes *live* est donc l'une des meilleures façons d'utiliser un ordinateur sans laisser de traces. Nous verrons ici comment obtenir un système *live*, et comment démarrer dessus.

Le moyen usuel d'utiliser un système *live* est de l'installer sur une clé USB, une carte SD ou de le graver sur un DVD. On parle dans ce cas de *Live DVD*.

Néanmoins, vu qu'il est possible d'écrire des données sur une clé USB ou une carte SD alors que ce n'est pas possible sur un DVD, après installation du système *live* on a moins de garanties au cas où les gens qui ont écrit le système *live* auraient commis des erreurs. Cela devient aussi plus simple pour des personnes malveillantes de modifier votre système *live* pour, par exemple, enregistrer vos mots de passe ou vos frappes au clavier.

14.2 Télécharger et installer Tails

On va expliquer ici comment télécharger la dernière version de Tails à partir de son site web officiel, vérifier son authenticité et l'installer sur une clé USB, une carte SD ou la graver sur un DVD.

page suivante

Si l'on dispose déjà de la dernière version de Tails, il est possible de la dupliquer simplement. Suivre pour cela l'outil [cloner Tails](#).

Pour télécharger et installer Tails, on va suivre la documentation officielle, disponible sur la page web <https://tails.boum.org/download/index.fr.html>.



plus bas

Attention : ce guide fournit des explications sur la vérification de l'intégrité de l'image de Tails. Lorsqu'on arrive à la section « Vérifier l'image ISO » de la documentation officielle de Tails, se rapporter à [vérifier son authenticité](#).

14.2.1 Télécharger Tails

Tails peut être téléchargé soit directement avec un navigateur web (en HTTP), soit à l'aide de BitTorrent.

BitTorrent est un protocole de partage de fichiers de pair-à-pair (« *peer-to-peer* » en anglais); il permet donc à tous les ordinateurs qui effectuent le téléchargement de participer à la diffusion des fichiers. Cela nécessite d'utiliser un logiciel dédié au téléchargement.

Quand cela est possible, cette méthode a l'avantage de garantir une certaine disponibilité des fichiers au cas où un problème arriverait sur les gros serveurs offrant le téléchargement direct. C'est donc celle-ci que nous allons développer.

plus bas

Si l'on choisit de télécharger l'image directement avec son navigateur web, on peut directement aller [vérifier son authenticité](#).

Télécharger le *torrent*

Pour télécharger en pair-à-pair, il faut tout d'abord télécharger un petit fichier, appelé *torrent*. Ce fichier contient les informations qui seront nécessaires au logiciel de téléchargement pour trouver les sources des fichiers que l'on veut obtenir.

On va donc télécharger le fichier Torrent en cliquant sur le bouton correspondant.

Télécharger l'image du système *live*

Sur une Debian standard, le logiciel de téléchargement de *torrents* *Transmission* démarrera automatiquement après le téléchargement du fichier torrent. Une fenêtre indiquant les fichiers qui seront téléchargés s'ouvre; après avoir vérifié le dossier de destination, il suffit de cliquer sur *Ouvrir* pour démarrer le téléchargement.

Si le client BitTorrent ne s'ouvre pas tout seul, on va l'ouvrir à la main :

page 120

- sous Debian ou Ubuntu, ouvrir le *Client BitTorrent Transmission*. Il peut être nécessaire, au préalable, d'[installer](#) le paquet `transmission-gtk`;
- sous Mac OS X, il est aussi possible d'installer *Transmission*¹;
- sous Windows, il est possible d'installer le client libre *Vuze*².

14.2.2 Vérifier l'authenticité du système *live*

tome 2 ch. 18

L'image du système *live* que l'on vient de télécharger est signée numériquement avec [OpenPGP](#).

1. <http://www.transmissionbt.com/>
2. <http://www.vuze.com/>

Après avoir téléchargé l'image ISO de la dernière version de Tails, ainsi que sa signature numérique, il va nous falloir vérifier son intégrité.

tome 2 § 6.3

Importer ensuite la clé OpenPGP qui signe les ISO de Tails :

tome 2 § 18.1

```
Tails developers (signing key) <tails@boum.org> 0xBE2CD9C1
```

tome 2 § 18.8

Vérifier la signature numérique de l'image ISO. L'empreinte observée par les auteurs de ce guide est, en admettant que c'est un exemplaire original que l'on a entre les mains :

```
0D24 B36A A9A2 A651 7878 7645 1202 821C BE2C D9C1
```

14.2.3 Installer Tails sur le support choisi

Retourner à la documentation officielle de Tails, disponible sur le site web section « Installer ou mettre à jour Tails » <https://tails.boum.org/download/index.fr.html#index5h1>.

Le fichier téléchargé est une « image ISO », c'est-à-dire un format de fichiers que la plupart des logiciels de gravure reconnaissent comme « image CD brute ». En général, si on insère un disque vierge ou réinscriptible dans son lecteur, qu'on fait un clic-droit sur le fichier téléchargé et qu'on choisit *Ouvrir avec Gravure de disque Brasero*, le logiciel de gravure s'occupe, après confirmation, de transformer cette image en l'écrivant sur le DVD.

14.3 Cloner ou mettre à jour une clé Tails

Une fois que l'on dispose d'un DVD, d'une clé USB ou d'une carte SD de Tails, il est possible de le dupliquer, par exemple pour créer une clé USB avec la persistance correspondant à une nouvelle identité contextuelle, pour donner une clé Tails à un ami, ou encore pour mettre à jour une clé USB contenant une ancienne version de Tails.

page ci-contre

Pour ce faire, on va suivre la documentation officielle de Tails, qui est disponible à partir de n'importe quel DVD, clé USB ou carte SD de Tails, même sans connexion à Internet.

plus bas

Démarrer Tails. Sur le bureau, cliquer sur l'icône *Documentation de Tails*. Dans le menu à droite, cliquer sur *Documentation*. Dans l'index qui s'ouvre, chercher la section *Premier pas avec Tails* et cliquer sur la page *Installation sur une clé USB ou une carte SD*. C'est celle-ci qu'il s'agira de suivre.

Pour mettre à jour la clé ainsi créée, il faudra par la suite suivre la page *Mettre à jour une Clé USB Tails ou une carte SD Tails* dans la même section.

14.4 Démarrer sur un système *live*

Dès que la copie ou la gravure est terminée, on peut redémarrer l'ordinateur en laissant le support du système *live* dedans, et vérifier que la copie a fonctionné... à condition bien sûr qu'on ait configuré le micrologiciel pour qu'il démarre sur le bon support : voir la recette expliquant comment démarrer sur un média externe pour les détails.

page 93

Au démarrage, Tails affiche un écran qui permet de choisir, entre autres options, la langue d'affichage et la disposition du clavier.

14.5 Utiliser la persistance de Tails

Lorsqu'on utilise Tails à partir d'une clé USB ou d'une carte SD, il est possible de créer un volume persistant chiffré sur l'espace libre de la clé créé par l'Installeur de Tails. [plus bas]

Les données contenues dans le volume persistant sont sauvegardées et restent disponibles d'une session de travail à l'autre. Le volume persistant permet de sauvegarder des fichiers personnels, des clés de chiffrement, des configurations ou des logiciels qui ne sont pas installés par défaut dans Tails.

[plus bas] Une fois le volume persistant créé, on peut choisir de l'activer, ou non, à chaque démarrage de Tails.

[plus bas] On pourra enfin le supprimer lorsqu'on ne voudra plus pouvoir accéder à ses données. L'utilisation d'un volume persistant n'est toutefois pas sans conséquences quant aux traces laissées. C'est pourquoi il faudra commencer par lire la page d'avertissements concernant l'usage de la persistance.

Pour cela, cliquer sur l'icône *Documentation de Tails* se trouvant sur bureau. Dans le menu à droite, cliquer sur *Documentation*. Dans l'index qui s'ouvre, chercher la section *Premier pas avec Tails* et cliquer sur la page *Avertissement à propos de la persistance*.

14.5.1 Créer et configurer un volume persistant

L'objectif de cette recette est de créer et de configurer un volume persistant sur une clé USB ou une carte SD de Tails.

[page préc.] Pour ce faire, on va suivre la documentation officielle de Tails, qui est disponible à partir de n'importe quel clé USB, carte SD ou DVD de Tails, même sans connexion à Internet.

Démarrer Tails. Sur le bureau, cliquer sur l'icône *Documentation de Tails*. Dans le menu à droite, cliquer sur *Documentation*. Dans l'index qui s'ouvre, chercher la section *Premier pas avec Tails* et cliquer sur la page *Persistance* et enfin *Créer et configurer un volume persistant*. Suivre cette page de documentation.

Si l'on a déjà un volume persistant et que l'on souhaite simplement modifier ses paramètres, aller directement à la section *Options du volume persistant*.

14.5.2 Activer et utiliser un volume persistant

L'objectif de cette recette est d'activer le volume persistant nouvellement créé sur une clé USB ou une carte SD de Tails.

[page préc.] Pour ce faire, on va suivre la documentation officielle de Tails, qui est disponible à partir de n'importe quel clé USB, carte SD ou DVD de Tails, même sans connexion à Internet.

Démarrer Tails. Sur le bureau, cliquer sur l'icône *Documentation de Tails*. Dans le menu à droite, cliquer sur *Documentation*. Dans l'index qui s'ouvre, chercher la section *Premier pas avec Tails* et cliquer sur la page *Persistance* et enfin *Activer et utiliser le volume persistant* et suivre cette page de documentation.

14.5.3 Supprimer un volume persistant

L'objectif de cette recette est de supprimer un volume persistant créé précédemment sur une clé USB ou une carte SD de Tails.

[page préc.] Pour ce faire, on va suivre la documentation officielle de Tails, qui est disponible à partir de n'importe quel clé USB, carte SD ou DVD de Tails, même sans connexion à Internet.

Démarrer *Tails*. Sur le bureau, cliquer sur l'icône *Documentation de Tails*. Dans le menu à droite, cliquer sur *Documentation*. Dans l'index qui s'ouvre, chercher la section *Premier pas avec Tails* et cliquer sur la page *Persistence* et enfin *Supprimer le volume persistant* et suivre cette page de documentation.

14.5.4 Installer un logiciel additionnel persistant dans Tails

Tails contient des logiciels adaptés à la plupart des tâches courantes lors de l'utilisation d'Internet et de la création de documents. Toutefois, pour des projets spécifiques, on peut avoir besoin d'installer un logiciel spécifique dans *Tails*, comme par exemple un logiciel de conception et de simulation de circuits électroniques.

Lorsque *Tails* est installé sur une clé USB ou sur une carte SD, il est possible de configurer un volume persistant pour qu'un ou plusieurs logiciels spécifiques soient installés de manière automatique à chaque démarrage.

Trouver le nom de paquet à installer On a besoin du nom exact du paquet à installer. Pour le trouver, suivre la recette [trouver un logiciel](#). Par exemple, notre logiciel de conception de circuits électroniques est fourni par le paquet `geda`.

page 116

Configurer les logiciels additionnels Si l'on ne dispose pas encore d'une clé USB ou d'une carte SD contenant un volume persistant, il faut en créer une grâce aux recettes [cloner une clé Tails](#) puis [créer et configurer un volume persistant dans Tails](#).

page 101

On suivra ensuite l'outil [créer et configurer un volume persistant dans Tails](#) pour activer les options *Paquets APT* et *Listes APT*.

page ci-contre

page ci-contre

Redémarrer alors *Tails*. Une fois redémarré, au niveau de l'écran d'accueil, après avoir choisi le français comme langue cliquer sur *Plus d'option ?* → *Oui*. Puis [activez la persistance](#). Maintenant cliquer sur *Suivant*. Choisir un *Mot de passe d'administration*, le rentrer deux fois et cliquer sur *Connexion*.

page ci-contre

Une fois sur le bureau, ouvrir un *Terminal administrateur* à partir du menu *Applications* → *Accessoires*. Entrer le mot de passe choisi précédemment puis *Valider*. Le terminal administrateur s'ouvre, taper dedans :



```
gedit /live/persistence/TailsData_unlocked/live-additional-software.conf
```

Puis taper sur *Entrer*.


Un fichier texte s'ouvre. Chaque ligne de ce fichier doit contenir le nom exact d'un paquet à installer. On va donc ajouter une ligne avec le nom du paquet trouvé précédemment. Dans notre exemple, on ajoutera la ligne :


```
geda
```

Enregistrer le fichier en cliquant sur *Enregistrer*. On peut maintenant fermer le fichier texte ainsi que le terminal et redémarrer *Tails*. Une fois [la persistance activée](#) et l'ordinateur connecté au réseau, notre logiciel devrait s'installer automatiquement au bout d'un temps plus ou moins long en fonction de la taille et du nombre de logiciels à installer (une fenêtre signale alors le succès de l'installation).

page ci-contre

Installer un système chiffré

 Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.

 *Durée* : compter une journée, avec plusieurs périodes d'attente (parfois longues).

On a vu que tout ordinateur — hormis avec certains systèmes *live* — laisse un peu partout des traces des fichiers ouverts, des travaux effectués, des connexions Internet, etc. On a vu aussi qu'une façon d'exposer un peu moins les données conservées sur l'ordinateur ainsi que les traces qu'on y laisse est de chiffrer le système sur lequel on travaille dans son ensemble.

[page 19]

[page 37]

Il est possible d'installer un système d'exploitation GNU/Linux comme Debian¹, sur une partie chiffrée du disque dur. À chaque démarrage, l'ordinateur va demander une phrase de passe, après quoi il débloque le chiffrement du disque, ce qui donne accès aux données, et permet donc le démarrage du système. Sans cette phrase, toute personne qui voudrait consulter le contenu de ce disque se trouvera face à des données indéchiffrables. C'est ce qu'on se propose de faire dans cette recette.

[page 15]

15.1 Limites



Attention ! Cette simple installation chiffrée ne règle pas tous les problèmes de confidentialité d'un coup de baguette magique. Elle ne protège les données qu'à certaines conditions.

15.1.1 Limites d'un système chiffré

Nous recommandons chaudement les lectures préalables suivantes :

- le chapitre concernant le chiffrement (et ses limites),
- le cas d'usage un nouveau départ, qui étudie, en détails, les limites pratiques d'un tel système et les attaques possibles contre lui.

[page 37]

[page 57]

Sans cela, l'installation d'un système chiffré peut procurer un sentiment erroné de sécurité, source de bien des problèmes.

15.1.2 Limites d'une nouvelle installation

Lors de l'installation d'un nouveau système, on part de zéro. Il n'y a aucun moyen simple de vérifier que le CD d'installation qu'on utilise est fiable, et ne contient pas

1. Pour chiffrer le disque dur lors de l'installation d'Ubuntu, il est nécessaire d'utiliser le CD nommé *alternate installer* [<http://www.ubuntu.com/download/ubuntu/alternative-download#alternate>].

par exemple de logiciels malveillants. On ne pourra éventuellement s'en rendre compte que *par la suite* — et peut-être qu'il sera trop tard...

15.1.3 Limites dans la prise en charge du matériel

Utiliser un système d'exploitation libre comme Debian a un désavantage : les fabricants de matériel y font généralement peu attention. Il arrive donc qu'il ne soit pas facile, voire complètement impossible, d'utiliser un ordinateur ou l'un de ses périphériques avec Debian.

page 13

La situation s'améliore depuis quelques années : le fonctionnement du matériel tend à s'homogénéiser, et surtout, la diffusion des systèmes libres pousse de plus en plus les fabricants à aider, directement ou non, à ce que leur matériel fonctionne².

Cependant, avant de remplacer un système d'exploitation, cela peut être une bonne idée de s'assurer que le matériel nécessaire fonctionne bien à l'aide d'un système *live*. Le système Tails, par exemple, est basé sur Debian. Le matériel qui fonctionne avec l'un devrait donc fonctionner avec l'autre sans difficultés.

page 99

15.2 Télécharger un support d'installation

Pour réaliser l'installation du système, le plus simple est d'utiliser un CD, un DVD ou une clé USB. Debian en propose plusieurs variantes, et il est donc nécessaire de commencer par choisir la méthode qui convient le mieux à notre situation.

15.2.1 Le CD d'installation par le réseau

Le plus rapide est d'utiliser un CD d'installation par le réseau. Le CD contient uniquement les tout premiers morceaux du système. Il télécharge ensuite, depuis Internet, les logiciels à installer. Il faut donc que l'ordinateur sur lequel on souhaite installer Debian soit connecté à Internet, de préférence par un câble réseau (et non par le *Wi-Fi* qui ne fonctionnera que rarement à l'intérieur du logiciel d'installation).

Il existe plusieurs fichiers (également appelés « images ») contenant une copie du CD d'installation, selon l'architecture du processeur. Dans la plupart des cas, il faudra télécharger celui dont le nom se termine par `amd64-i386-netinst.iso`, dit multi-architecture³, qui conviendra pour les architectures 32 et 64 bits.

page 10

Cette image fonctionnera sur la plupart des ordinateurs domestiques fabriqués après 2006⁴.

15.2.2 Le DVD avec l'environnement graphique

S'il n'est pas possible de connecter à Internet l'ordinateur sur lequel on souhaite installer Debian, il est possible de télécharger un DVD contenant tout le système de base ainsi que l'environnement graphique habituel. Cela nécessite d'avoir accès à un graveur de DVD ou à une clé USB d'au moins 4GB.

2. Pour certains matériels, des problèmes peuvent venir de défauts dans le fonctionnement des microcodes intégrés. Ces problèmes sont parfois corrigés par des mises à jour que fournissent les fabricants. Cela peut donc être une bonne idée de faire les mises à jour du micrologiciel (BIOS ou UEFI), de l'*Embedded Controller* ou d'autres composants avant de procéder à l'installation. Malheureusement, ces procédures diffèrent trop d'un matériel à un autre pour être détaillées dans cet ouvrage, mais peuvent en général être trouvées sur le site du constructeur...

3. Les images multi-architectures d'installation par le réseau sur le site de Debian [<http://cdimage.debian.org/debian-cd/current/multi-arch/iso-cd/>]

4. Pour les « vieux » Macs (*iBook G4* par exemple), il est nécessaire d'utiliser l'image dont le nom se termine par `powerpc-netinst.iso` que l'on trouvera sur le même site [<http://cdimage.debian.org/debian-cd/current/powerpc/iso-cd/>]. À noter : il n'est pas possible de créer une clé USB à partir de cette image, il vous faudra donc utiliser un DVD.

De la même manière que pour l'installation par le réseau, on choisira le DVD correspondant à notre architecture. Le DVD d'installation multi-architecture⁵ devrait convenir pour la plupart des ordinateurs.

Seul le premier DVD est nécessaire pour réaliser l'installation. Le nom du fichier à télécharger devrait ressembler `debian-7.4.0-i386-amd64-source-dvd-1.iso`.

15.2.3 Utiliser une clé USB

Le système d'installation de Debian permet de transférer le contenu du CD d'installation par le réseau, ou celui du DVD, sur une clé USB dédiée à cela. On peut ainsi installer Debian sur un ordinateur n'ayant pas de lecteur CD ou DVD.

Transférer le DVD demande une clé d'une capacité de plus de 5 Go. Le CD d'installation par le réseau nécessite quant à lui une capacité de 512 Mo. Attention, cette opération nécessite l'utilisation de l'intégralité de la clé USB. Il faudra donc veiller à sauvegarder auparavant les fichiers qui s'y trouvent.

15.3 Vérifier l'empreinte du support d'installation

Il est bon de s'assurer que le téléchargement de l'image s'est bien déroulé en vérifiant l'empreinte de l'installateur, pour s'assurer de son intégrité et de son authenticité. Nous allons procéder en deux étapes, une première nous assurant de son intégrité, et une seconde assurant son authenticité.

[page 37]

Pour cela, il est nécessaire de démarrer sur un système déjà installé. Si l'on a accès à un ordinateur sous GNU/Linux, tout va bien. Si on ne dispose que d'un système live, il est par exemple possible de mettre l'image téléchargée sur une clé USB, puis de vérifier l'empreinte à partir du système *live*.

[page 99]

15.3.1 Vérifier l'intégrité du support d'installation

Pour cela suivre l'outil concernant les sommes de contrôle. Il sera nécessaire de calculer la somme de contrôle SHA512 du support d'installation téléchargé et vérifier si celle-ci correspond à celle contenue dans le fichier `SHA512SUMS` contenu dans le même dossier que le support d'installation. Fichier que l'on devra télécharger également.

[page 153]

15.3.2 Vérifier l'authenticité du support d'installation

Si la vérification de l'intégrité s'est bien déroulée, à savoir si les deux sommes de contrôles calculées correspondent, on peut poursuivre le processus afin de vérifier son authenticité. En effet, un adversaire pourrait fournir un support d'installation corrompu et sa somme de contrôle. La vérification précédente nous permettrait simplement de constater que le fichier téléchargé est bien celui qui était disponible sur le site web, pas qu'il est celui qu'on espère avoir. Le deuxième tome explique comment s'assurer de l'authenticité de l'installateur téléchargé, car l'empreinte est signée avec GnuPG, qui utilise la cryptographie asymétrique, il faudra donc directement se référer à l'outil concernant la vérification d'une signature. Après avoir téléchargé le fichier `SHA1SUMS.sign`, suivre les étapes permettant de vérifier la signature cryptographique du fichier `SHA512SUMS`.

[tome 2 § 18.8]

15.4 Préparer les supports d'installation

Une fois l'image du support d'installation choisie et téléchargée et vérifiée, il nous reste à la transférer sur un CD, un DVD ou une clé USB.

⁵. Les DVD d'installation de Debian multi-architecture [<http://cdimage.debian.org/debian-cd/current/multi-arch/iso-dvd/>]

15.4.1 Graver le CD ou le DVD d'installation

Le fichier téléchargé est une « image ISO », c'est-à-dire un format de fichiers que la plupart des logiciels de gravure reconnaissent comme « image CD brute ». En général, si on insère un disque vierge dans son lecteur, qu'on fait un clic-droit sur le fichier et qu'on choisit *Gravure de disque Braseo*, le logiciel de gravure s'occupe tout seul de transformer cette image en l'écrivant sur le disque vierge — en tout cas, ça marche avec Tails, et plus généralement sous Debian ou Ubuntu.

Sous Windows, si on a pas déjà installé de logiciel capable de graver des images ISO, le logiciel libre InfraRecorder⁶ fera parfaitement l'affaire.

15.4.2 Créer une clé USB d'installation

page 99

Pour créer une clé USB d'installation, il est nécessaire d'effectuer les opérations qui suivent à partir d'un système basé sur Linux tel que Debian ou Tails.

Se munir d'une clé USB vierge, ou contenant uniquement des données auxquelles on ne tient pas.



page 32

Attention : les données éventuellement présentes sur la clé seront perdues. Par contre, il serait facile de procéder à une analyse pour retrouver les fichiers dont le contenu n'aurait pas été écrasé auparavant...

Repérer l'emplacement de la clé USB

Pour la suite des opérations, il est nécessaire de déterminer le nom que le système attribue à la clé USB. Pour ce faire, on va démarrer l'*Utilitaire de disque* dans le menu *Applications* → *Accessoires*.

Une fois ce dernier ouvert, on peut brancher notre clé USB. Une entrée correspondant à cette dernière devrait apparaître dans la liste située à gauche. Après l'avoir sélectionnée, on pourra lire le *nom* du disque dans la partie à droite, sous l'intitulé *Disque*, à côté de l'étiquette *Périphérique*.

Cela doit ressembler à `/dev/sdx` : c'est ainsi que l'ordinateur a identifié le support de stockage que l'on vient de brancher. C'est le nom qu'on devra écrire par la suite dans certaines commandes, à la place de `LE_PÉRIPHERIQUE`.

Comme on va remplacer ce qui se trouvait sur la clé, il faut également demander au système de ne plus utiliser ce qu'elle contient : toujours dans la partie droite, on sélectionne donc, tour à tour, chacun des *Volumes* dessinés. Pour chacun d'entre eux, on clique sur *Démonter le volume* si ce bouton est disponible. S'il s'agit d'une partition chiffrée, il nous faudra également cliquer juste au dessus, sur la partie intitulée « Chiffré », puis sur le bouton *Verrouiller le volume*.

Plutôt que de fermer l'*Utilitaire de disque* dès maintenant, mieux vaut réduire sa fenêtre : on en aura encore besoin une dernière fois après la copie proprement dite.

Lancer la copie brute

page 85

On va maintenant ouvrir un *Terminal*, tout en gardant à portée de souris l'icône de l'image ISO téléchargée auparavant.

On va commencer la commande en tapant (**sans** faire *Entrée*) :



```
cat
```

6. <http://infrarecorder.org/>

Ajouter ensuite un espace. Puis, on va indiquer la *source* de la copie (la chose que l'on va copier). Pour ce faire, il faut, avec la souris, cliquer sur l'icône du fichier ISO que l'on vient de télécharger puis de vérifier et le faire glisser dans la fenêtre du terminal. Après avoir relâché le bouton, ce qui est affiché doit ressembler à :

```
$> cat '/home/domi/Desktop/debian-7.4.0-amd64-i386-netinst.iso'
```

Ce n'est toujours pas fini, car il faut maintenant indiquer la *destination* de la copie, en ajoutant à la fin de notre commande :

```
$> > LE_PÉRIPHÉRIQUE
```

Une fois cela fait, la commande complète doit ressembler à quelque chose comme :

```
$> cat '/home/domi/Desktop/debian-7.4.0-amd64-i386-netinst.iso' > /dev/sdx
```

La copie se lance dès qu'on a appuyé sur *Entrée*, ne laissant plus apparaître qu'un sobre carré à la ligne suivante.

Après de la patience et le retour du signe # symbolisant l'invite de commande, on peut fermer le terminal. Reste ensuite à faire réapparaître la fenêtre de l'*Utilitaire de disque* et à cliquer sur *Déconnexion en toute sécurité* pour être sûr de ne pas abîmer les données fraîchement copiées sur notre clé USB.

15.4.3 Mettre les « microcodes » sur une clé USB

Certains périphériques de l'ordinateur peuvent nécessiter, pour fonctionner, que le système leur fournisse un « microcode » (ou *firmware*)... mais ce n'est pas toujours le cas. [page 13]

On peut donc tenter de réaliser l'installation sans s'en préoccuper et revenir lire cette section plus tard si l'on rencontre des problèmes.

Un micro—quoi ?

Ces microcodes sont des programmes qui ont la particularité de s'exécuter sur des puces électroniques à l'intérieur du périphérique et non sur le processeur de l'ordinateur. C'est par exemple le cas du programme qui contrôlera le déplacement des parties mécaniques d'un disque dur ou le fonctionnement du système de radio d'une carte Wi-Fi. On ne se rend pas forcément compte qu'ils existent... car la plupart des microcodes sont livrés directement avec le matériel. [page 10]

Mais pour d'autres périphériques, le système d'exploitation doit envoyer le microcode à un composant lors de son initialisation.

Ceux qui sont libres sont livrés avec le programme d'installation de Debian. Malheureusement, la plupart des microcodes ne sont pas libres. Nous devons donc mettre nous-mêmes à disposition du programme d'installation tout microcode non-libre nécessaire au fonctionnement de l'ordinateur : c'est typiquement le cas pour certaines cartes Wi-Fi. [page 29]

Même si c'est hautement improbable, on peut envisager que le microcode propriétaire d'une carte Wi-Fi nous espionne à notre insu... sauf que sans microcode, elle ne fonctionnera tout simplement pas. C'est encore une fois une histoire de compromis.

Obtenir les microcodes supplémentaires

Une bonne partie des microcodes non-libres sont néanmoins redistribués par le projet Debian.

Ils sont livrés dans une archive nommée `firmware.tar.gz`, que l'on peut télécharger sur la page : <http://cdimage.debian.org/cdimage/unofficial/non-free/firmware/wheezy/current/>

Utiliser une clé USB en plus d'un CD ou d'un DVD

Si on utilise un CD ou un DVD pour réaliser l'installation, il est nécessaire de copier les microcodes supplémentaires sur une clé USB. Il est possible d'utiliser une clé USB contenant déjà des données, mais cette clé ne doit pas être chiffrée.

Pour cela, il faut créer dans la clé un nouveau répertoire que l'on baptisera `firmware`⁷, et y extraire (avec le *Gestionnaire d'archives*) le contenu de l'archive que l'on vient de télécharger.

Pour ce faire, il suffit (avec un système GNU/Linux) de double-cliquer sur le fichier `firmware.tar.gz` qu'on vient de télécharger. Le *Gestionnaire d'archives* s'ouvre : cliquer sur le bouton *Extraire* dans le menu du haut, et choisir ensuite comme emplacement le dossier `firmware` de la clé USB en question. On peut ensuite démonter la clé.

Utiliser une seule clé USB

Si on réalise l'installation à partir d'une clé USB, il est possible de copier les microcodes sur cette même clé.

Pour cela, il faut commencer par ouvrir l'*Utilitaire de disque* à partir du menu *Applications* → *Accessoires*. Puis :

- brancher la clé USB dans l'ordinateur ;
- sélectionner la clé USB dans la liste de gauche ;
- dans la partie droite, cliquer sur la zone indiquée comme *Libre* sous l'intitulé *Volumes* ;
- cliquer sur le bouton *Créer une partition* en-dessous ;
- choisir *FAT* comme *Type* et `firmware` comme nom ;
- cliquer sur le bouton *Créer*.

On peut maintenant fermer l'*Utilitaire de disque*, utiliser le *Gestionnaire d'archives* pour extraire le contenu de l'archive téléchargée précédemment sur l'espace de la clé USB s'appelant `firmware`, et démonter cette dernière.

15.5 L'installation proprement dite

page 93

Pour installer la Debian chiffrée depuis le support d'installation (CD, DVD ou clé USB), il faut démarrer sur celui-ci en suivant la recette correspondante.

À partir de là, l'installation proprement dite peut commencer : prévoir du temps devant soi et quelques mots croisés, car l'ordinateur pourra travailler longtemps sans surveillance particulière.

Vérifier, dans le cas d'un CD d'installation par le réseau, que le câble reliant l'ordinateur au réseau est bien branché. Et s'il s'agit d'un ordinateur portable, vérifier que le câble d'alimentation est branché, car il n'y a pas de notification de batterie faible durant l'installation.

7. Le nom du répertoire doit *vraiment* être `firmware`, sinon cela ne marchera pas.

Le programme d'installation de Debian dispose de sa propre documentation⁸. En cas de doute à la lecture des étapes décrites par la suite, cela peut valoir le coup d'y jeter un œil. Par ailleurs, pour la plupart des choix qu'il nous demande de faire, le programme d'installation nous proposera automatiquement une réponse qui fonctionne généralement...

15.5.1 Lancement de l'installateur

On démarre donc sur le support d'installation (CD, DVD ou clé USB). Un premier menu nommé *Debian GNU/Linux installer boot menu* apparaît.

Dans le cas où on a choisi un CD multi-architecture, certaines options seront présentes en double, marquées comme « 64-bit ».

L'option sélectionnée automatiquement par l'installateur sera soit *Install*, soit *64-bit install*; dans ce dernier cas, le programme d'installation a détecté que le processeur est compatible avec l'architecture `amd64`, qui apporte quelques avantages en termes de sécurité.

page 10

Il est plus commode d'utiliser la souris lors de l'installation ; on choisira donc *Graphical install*, dans le cas où *Install* était pré-sélectionné, et plutôt *64-bit graphical install*, si *64-bit install* avait été sélectionné tout seul. Ce choix s'effectue en se déplaçant avec les touches `↓` et `↑` du clavier.

Une fois la bonne ligne sélectionnée, il faut appuyer sur la touche *Entrée* pour lancer la suite du programme d'installation.

15.5.2 Choisir la langue et la disposition du clavier

- Après un peu de patience, un menu nommé *Select a language* apparaît : l'installateur propose de choisir une langue pour la suite de l'installation. Toujours en se déplaçant avec les flèches, sélectionner *Français* et appuyer sur la touche *Entrée*.
- Un menu demande le pays, pour peaufiner l'adaptation du système. Choisir son lieu géographique, et appuyer sur *Entrée*.
- Dans *Configurer le clavier*, le choix par défaut *Français* convient si l'on a un clavier français « azerty ».
- L'installateur charge ensuite les fichiers dont il a besoin.

15.5.3 Configuration du réseau et baptême de la machine

- L'installateur prend alors un peu de temps pour configurer le réseau. Si notre ordinateur possède plusieurs cartes réseau, il faut choisir celle dont on va se servir pour l'installation. Le choix par défaut est généralement le bon, il s'agit d'une carte réseau *Ethernet*. On nous demande ensuite le *Nom de machine*. Choisir un petit nom pour son ordinateur, en sachant que ce nom sera ensuite visible depuis le réseau, et pourra aussi s'inscrire dans les fichiers créés ou modifiés avec le système qu'on est en train d'installer.
- L'installateur demande le *Domaine*. Sans entrer dans les détails, mieux vaut laisser ce champ vide (donc effacer ce que le programme peut éventuellement avoir pré-rempli).

15.5.4 Créer les utilisateurs et choisir les mots de passe

Le programme d'installation nous demande maintenant de choisir le *mot de passe du superutilisateur*. C'est ce mot de passe qui sera nécessaire pour réaliser les tâches

8. Le manuel d'installation est disponible dans de nombreuses versions [<http://www.debian.org/releases/wheezy/installmanual.fr.html>]. On suivra celui correspondant à l'architecture du processeur [page 10].

d'administration de l'ordinateur : mises à jour, installation de logiciels, modifications majeures du système, *etc.*

Il est toutefois possible de s'épargner un mot de passe supplémentaire, et de permettre que le premier compte créé sur le système ait le droit de faire des opérations d'administration⁹. Pour cela, il suffit de ne pas entrer de mot de passe pour le super-utilisateur : laisser simplement la case vide.

Cela dit, ce choix doit être bien pesé au préalable : souvent, il est plus simple d'utiliser cette méthode, notamment parce qu'il n'y a pas un mot de passe supplémentaire à retenir. Cependant, dans sa configuration par défaut, elle peut permettre à n'importe quel programme lancé dans ce compte, *sans que celui-ci nous demande confirmation au préalable*, d'effectuer des opérations en disposant des privilèges d'administrateur ; et ce, pendant quinze minutes après la saisie du mot de passe.

- Dans *Nom complet du nouvel utilisateur* choisir le nom associé au premier compte créé sur le système. Ce nom sera souvent enregistré dans les documents créés ou modifiés dans cette session ; il peut donc être intéressant de choisir un nouveau pseudonyme.
- Dans *Identifiant pour le compte utilisateur*, choisir un identifiant (*login*) pour ce compte. Il est prérempli, mais peut être modifié. L'installateur prévient, pour le cas où l'on voudrait le changer, qu'il doit commencer par une lettre minuscule et être suivi d'un nombre quelconque de chiffres et de lettres minuscules.
- L'installateur demande un mot de passe pour l'utilisateur qui aura le droit d'administrer l'ordinateur, si l'on a décidé de ne pas entrer un mot de passe « superutilisateur » précédemment.

15.5.5 Partitionner les disques

Le CD démarre ensuite l'outil de partitionnement. Il détecte les partitions présentes, et va proposer de les modifier.

- Dans le menu *Méthode de partitionnement*, choisir *Assisté — utiliser tout un disque avec LVM chiffré*.
- Dans *Disque à partitionner* choisir le disque sur lequel installer Debian GNU/Linux. Si l'on veut supprimer le système actuellement installé, il correspond en général au premier disque de la liste. La taille du disque est un indice permettant de ne pas se tromper, pour ne pas essayer d'installer Debian sur la clé USB contenant l'installateur par exemple.
- L'installateur propose ensuite différents *Schémas de partitionnement*. Là, il y a plusieurs possibilités :
 - *Tout dans une seule partition* fonctionne toujours ;
 - si l'on a un gros disque (pas moins de 20 Go), on peut décider de stocker le répertoire */home*, qui contiendra vos données personnelles, dans une partition séparée.
- L'installateur prévient alors qu'il va appliquer le schéma actuel de partitionnement, ce qui sera irréversible. Vu que l'on a bien fait les sauvegardes de ce que l'on voulait garder, répondre *Oui à Écrire les modifications sur les disques et configurer LVM ?*
- L'installateur va alors remplacer l'ancien contenu du disque par des données aléatoires. C'est très long — de nombreuses heures sur un gros disque — et ça laisse donc du temps pour faire autre chose !
- L'installateur demande alors une *Phrase secrète de chiffrement*. Choisir une bonne phrase de passe et la taper.
- Confirmer la phrase de passe en la tapant une seconde fois.
- L'installateur montre une liste de toutes les partitions qu'il va créer. Il est possible de lui faire confiance et de *Terminer le partitionnement et appliquer les changements*.

9. Ce mode est appelé *sudo*, car dans le terminal, il sera possible, en ajoutant *sudo* au début de la ligne, d'exécuter une commande en tant que « superutilisateur ».

- L'installateur prévient qu'il va détruire toutes les données présentes sur le disque. Tout le disque a déjà été rempli de données aléatoires, donc s'il contenait des données importantes elles ont déjà été effacées. Répondre *Oui* à *Faut-il appliquer les changements sur les disques ?* L'installateur crée alors les partitions, ce qui peut prendre un petit bout de temps.

15.5.6 Installation du système de base

L'installateur va maintenant installer un système GNU/Linux minimal. Le laisser faire...

15.5.7 Choix du serveur Debian

Si cette question n'apparaît pas à ce moment, pas d'inquiétude, c'est simplement que l'installateur utilisé n'est pas celui par le réseau. Dans ce cas, elle arrivera un peu plus tard au cours de l'installation.

- L'installateur demande de choisir le *Pays du miroir de l'archive Debian*. Le choix par défaut *France* est bon si l'on est en France.
- Il demande ensuite le *Miroir de l'archive Debian* à utiliser. Le choix par défaut *ftp.fr.debian.org* est aussi très bien.
- L'installateur demande si on a besoin d'un *Mandataire HTTP*. On laisse vide.
- L'installateur télécharge alors les fichiers dont il a besoin pour continuer.

15.5.8 Sélection des logiciels

La prochaine question concerne la *configuration de popularity-contest* et demande *Souhaitez-vous participer à l'étude statistique sur l'utilisation des paquets ?* Il est possible de répondre *Oui* sans risque de divulguer beaucoup d'informations supplémentaires : vu que les logiciels seront de toute façon téléchargés à partir des serveurs de Debian, ceux-ci pourraient déjà savoir quels paquets on utilise s'ils le voulaient.

L'installateur demande quels sont les *Logiciels à installer*. Ses propositions conviennent en général : *environnement de bureau Debian*, *serveur d'impression* et *Utilitaires usuels du système*, plus *ordinateur portable* le cas échéant.

L'installateur télécharge alors tout le reste du système Debian GNU/Linux et l'installe. C'est long, il y a le temps d'aller faire autre chose.

15.5.9 Installation du programme de démarrage GRUB

L'installateur propose de mettre en place le programme de démarrage, qui permet de démarrer Linux, sur une partie du disque dur appelée « secteur d'amorçage ». L'installateur propose un *Périphérique où sera installé le programme de démarrage*, laisser le choix par défaut, cliquer sur *Continuer* et attendre un peu.

Lorsqu'il a terminé, l'installateur propose de redémarrer l'ordinateur en vérifiant que le support d'installation (CD, DVD, clé USB) n'est plus inséré lors du redémarrage. Choisir *Continuer*.

15.5.10 Redémarrer sur le nouveau système

L'ordinateur démarre alors sur le nouveau système. À un moment, il demande la phrase de passe sur un écran noir : « **Enter passphrase:** ». La taper, sans s'inquiéter que rien ne s'affiche, et appuyer sur la touche *Entrée* à la fin¹⁰.

10. Si l'on n'est pas très à l'aise avec la frappe au clavier, il arrive souvent dans les premiers temps qu'on fasse une erreur de frappe dans la phrase, et c'est d'autant plus probable qu'aucun caractère ne s'affiche. Ne pas s'inquiéter des erreurs répétées, et insister jusqu'à réussir à taper la phrase sans faute... au bout de quelque temps, elle sera « rentrée dans les doigts », et les fautes de frappe se feront plus rares. Cela dit, il ne coûte rien de vérifier qu'on n'a pas malencontreusement laissé la

Après le démarrage d'un certain nombre de programmes, un écran apparaît avec le nom de la machine et le nom du compte utilisateur entré précédemment. Il faut sélectionner ce dernier, puis entrer le mot de passe associé.

Voilà un nouveau système Debian chiffré prêt à être utilisé. Pour qui n'en aurait jamais utilisé, se balader dedans peut être une bonne idée pour s'y familiariser. En haut de l'écran, le menu *Applications* permet d'accéder aux nombreux logiciels déjà installés. Les pages d'aide contenant de nombreux conseils et astuces sont accessibles à travers le menu *Applications* → *Accessoires* → *Aide*.

15.6 Quelques pistes pour continuer

- page 143 : Il peut maintenant être utile d'apprendre à sauvegarder des données... et à en effacer « pour de vrai ».
- page 127 : Il est également important d'apprendre à garder son système à jour. Des problèmes affectant les logiciels sont découverts régulièrement, et il est important d'installer les corrections au fur et à mesure de leur disponibilité.
- page 169 :

15.7 Un peu de documentation sur Debian et GNU/Linux

Voici quelques références de documentations sur Debian et GNU/Linux :

- Le guide de référence officiel de Debian ¹¹ ;
- La page d'accueil de la documentation officielle d'utilisation de Debian ¹² ;
- La Formation Debian GNU/Linux ¹³ : une excellente auto-formation sur Debian en français ;
- Le cahier de l'administrateur Debian ¹⁴.

On peut trouver beaucoup de documentation sur l'utilisation de GNU/Linux. Si elles sont souvent très utiles, elles sont malheureusement, comme beaucoup de choses sur Internet du reste, de qualité inégale. En particulier, beaucoup d'entre elles arrêteront de fonctionner lorsqu'une partie du système sera modifiée, ou seront peu soucieuses de l'intimité que l'on attend de notre système. Il faut donc faire preuve d'esprit critique et tenter de les comprendre avant de les appliquer.

Ceci dit, voici encore quelques références de wikis et des forums :

- Le wiki officiel de Debian ¹⁵ (partiellement traduit de l'anglais) ;
- Le forum en français sur Debian debian-fr.org ¹⁶ ;
- Andesi ¹⁷ : un wiki et forum en français sur Debian.

touche VerrMaj enfoncée, auquel cas l'on pourrait s'acharner longtemps sur le clavier sans pour autant arriver à déverrouiller le disque dur.

11. <http://www.debian.org/doc/manuals/debian-reference/index.fr.html>

12. <http://www.debian.org/doc/user-manuals>

13. <http://formation-debian.via.ecp.fr/>

14. <http://debian-handbook.info/browse/fr-FR/stable/>

15. <http://wiki.debian.org/>

16. <http://forum.debian-fr.org/>

17. <http://www.andesi.org/>

Choisir, vérifier et installer un logiciel

Cette partie propose quelques recettes à propos de la gestion de ses logiciels :

- Comment trouver un paquet Debian ? Lorsqu'on cherche à réaliser de nouvelles tâches avec un ordinateur, on est souvent amené à installer de nouveaux logiciels... quelques conseils pour trouver ce que l'on cherche dans Debian ; [page suivante]
- Avec quels critères de choix ? On doit parfois choisir un logiciel pour effectuer une certaine tâche, et il est alors courant de se sentir perdu dans la multitude de solutions disponibles... quelques critères permettant de prendre une décision adéquate ; [page 117]
- Comment installer un paquet Debian ? Une fois que l'on sait quel paquet contient le logiciel que l'on veut utiliser, reste à l'installer proprement ; [page 120]
- Comment modifier ses dépôts Debian ? Les paquets Debian qui contiennent les programmes se trouvent dans ce qu'on appelle des *dépôts*. Si les dépôts fournis avec Debian contiennent quasiment tous les logiciels dont on peut avoir besoin, il est parfois utile d'ajouter de nouveaux dépôts. [page 122]

16.1 Trouver un logiciel

🔄 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

🕒 *Durée : de 5 minutes (si l'on connaît le nom du logiciel que l'on cherche) à une demi-heure (si l'on part de zéro).*

Parfois, on connaît déjà le nom du logiciel que l'on souhaite installer — parce qu'on nous l'a conseillé, parce qu'on l'a trouvé sur Internet — et l'on veut savoir s'il est dans Debian. D'autres fois, on connaît seulement la tâche que l'on souhaiterait que le logiciel remplisse. Dans tous les cas, la base de données des logiciels disponibles dans Debian répondra certainement à nos questions.

Pour faire des choix éclairés, lorsque plusieurs logiciels permettent d'effectuer une même tâche, voir choisir un logiciel.

page ci-contre

- Ouvrir le *gestionnaire de paquets Synaptic* à partir du menu *Applications* → *Outils système* → *Administration*. Puisque le gestionnaire de paquets permet de modifier les logiciels installés sur l'ordinateur, et donc de choisir à quels programmes on fait confiance, on est rassuré qu'il nous demande notre mot de passe pour s'ouvrir.
- Une fois dans le gestionnaire de paquets, commençons par recharger la liste des paquets disponibles en cliquant sur l'icône *Recharger*. Le gestionnaire de paquets télécharge alors les dernières informations sur les paquets disponibles depuis un serveur Debian.
- Ensuite, il y a deux techniques pour chercher un paquet :
 - soit cliquer sur l'icône *Rechercher* dans la barre d'outils. Là, vérifier que *Description et nom* est bien sélectionné dans *Rechercher dans*. Taper des mots-clé ou un nom d'application dans la case *Rechercher* (par exemple « dictionnaire allemand openoffice »). Les descriptions des applications peu courantes sont rarement traduites en français. Avec quelques bases d'anglais, il est souvent intéressant d'essayer des mots-clé dans cette langue. Cliquer sur *Rechercher* pour lancer la recherche ;
 - soit sélectionner une catégorie dans la colonne de gauche.
- Les résultats de la recherche ou les paquets de la catégorie s'affichent alors dans la liste en haut à droite. En cliquant sur le nom d'un paquet, sa description apparaît dans le cadre en bas à droite.
- Reste maintenant à installer le paquet correspondant.

page 120

16.2 Critères de choix

🔄 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

🕒 *Durée : une demi-heure à une heure.*

On est parfois amené à choisir un logiciel pour effectuer une certaine tâche, et il est alors courant de se sentir perdu dans la multitude de solutions disponibles. Voici donc quelques critères permettant de prendre une décision adéquate.

L'intérêt d'utiliser des logiciels libres par rapport à des logiciels propriétaires ou *open source* a d'ores et déjà été expliqué. La suite du texte s'attachera donc uniquement à partager les logiciels libres disponibles.

page 29

16.2.1 Mode d'installation

Il est généralement préférable d'installer des logiciels fournis par sa distribution GNU/Linux (par exemple, Debian). Il y a deux principales raisons à ça.

Tout d'abord, une question pratique : la distribution fournit les outils pour installer et mettre à jour, de façon plus ou moins automatisée, un ensemble de logiciels ; elle nous alerte lorsqu'une faille de sécurité affecte l'un des logiciels que l'on utilise. Mais dès lors qu'on installe un logiciel qui n'est pas fourni par sa distribution, on est livré à soi-même : il faut penser à le mettre à jour, se tenir informé des failles de sécurité qui y sont découvertes, gérer les dépendances entre logiciels. Ça demande des efforts, du temps, des compétences.

D'autre part, une question de politique de sécurité : lorsqu'on a choisi sa distribution GNU/Linux, on a implicitement décidé d'accorder une certaine confiance à un ensemble de gens, à un processus de production. Installer un logiciel qui n'est pas fourni par sa distribution implique de prendre une décision similaire à propos d'un nouvel ensemble de gens, d'un nouveau processus de production. Une telle décision ne se prend pas à la légère : lorsqu'on décide d'installer un logiciel n'appartenant pas à sa distribution, on élargit l'ensemble des personnes et processus à qui on accorde de la confiance, et on augmente donc les risques.

16.2.2 Maturité

L'attrait de la nouveauté qui lave plus blanc que blanc est bien souvent un piège.

Mieux vaut, autant que possible, choisir un logiciel ayant atteint une certaine maturité : dans un logiciel activement développé et utilisé depuis au moins quelques années, il y a des chances que les plus gros problèmes aient déjà été découverts et corrigés... y compris les failles de sécurité.

Pour s'en rendre compte, il faut consulter l'historique de chacun des logiciels, sur leur site web ou dans le fichier nommé `ChangeLog` (ou `approchant`), généralement livré avec le logiciel.

16.2.3 Processus de production et « communauté »

L'étiquette *logiciel libre* est un critère essentiellement juridique, qui ne doit jamais suffire à nous inspirer confiance.

page 30

Certes, le fait qu'un logiciel soit placé sous une licence libre ouvre la possibilité de modes de développement inspirant confiance.

Mais les personnes développant ce logiciel peuvent fort bien, intentionnellement ou non, décourager toute coopération et travailler en vase clos. Que nous importe alors

que le programme soit *juridiquement* libre, si, de fait, personne d'autre ne lira jamais son code source ?

Il convient donc d'étudier rapidement le processus de production des logiciels en lice, en s'aidant des questions suivantes, qui nous permettront de surcroît de jauger le dynamisme du processus :

- Qui développe ? Une personne, des personnes, toute une équipe ?
- Le nombre de personnes qui contribuent au code source va-t-il en augmentant ou en diminuant ?
- Le développement est-il actif ? Il ne s'agit pas ici de vitesse pure, mais de réactivité, de suivi à long terme, de résistance. Le développement logiciel est une course d'endurance et non un *sprint*.

Et à propos des outils de communication collective sur lesquels s'appuie le développement (listes et salons de discussion, par exemple) :

- A-t-on facilement accès aux discussions guidant le développement du logiciel ?
- Ces discussions rassemblent-elles de nombreuses personnes ?
- Ces personnes participent-elle à son développement, ou ne font-elles que l'utiliser ?
- Quelle atmosphère y règne ? Calme plat, silence de mort, joyeuse cacophonie, sérieux glaçant, bras ouverts, hostilité implicite, tendre complicité, *etc.* ?
- Le volume de discussion, sur les derniers mois/années, va-t-il en diminuant ou en augmentant ? Plus que le volume brut, c'est surtout la proportion de messages obtenant des réponses qui importe : un logiciel mûr, stable et bien documenté ne sera pas forcément source de discussions, mais si plus personne n'est là pour répondre aux questions des néophytes, ça peut être mauvais signe.
- Peut-on trouver des retours d'utilisation, des suggestions d'améliorations ? Si oui, sont-elles prises en compte ?
- Les réponses sont-elles toujours données par un nombre réduit de personnes, ou existe-t-il des pratiques d'entraide plus large ?

16.2.4 Popularité

La popularité est un critère délicat en matière de logiciels. Le fait que la grande majorité des ordinateurs de bureau fonctionnent actuellement sous Windows n'indique en rien que Windows soit le meilleur système d'exploitation disponible.

Pour autant, si ce logiciel n'est pas utilisé par beaucoup de monde, on peut douter de sa viabilité à long terme : si l'équipe de développement venait à cesser de travailler sur ce logiciel, que deviendrait-il ? Qui reprendrait le flambeau ?

On peut donc retenir, comme règle générale, qu'il faut choisir un logiciel utilisé par un nombre suffisamment important de personnes, mais pas forcément *le* logiciel le plus utilisé.

Afin de mesurer la popularité d'un logiciel, il est possible, d'une part, d'utiliser les mêmes critères que ceux décrits ci-dessus au sujet du dynamisme de la « communauté » formée autour de lui. D'autre part, Debian publie les résultats de son concours de popularité¹, qui permet de comparer non seulement le nombre de personnes ayant installé tel ou tel logiciel, mais aussi, voire surtout, l'évolution dans le temps de leur popularité.

16.2.5 Passé de sécurité

Voici de nouveau un critère à double tranchant.

1. Debian.org, 2014, *Debian Popularity Contest* [<http://popcon.debian.org/>] (en anglais).

On peut commencer par jeter un œil sur le suivi de sécurité² proposé par Debian. En y cherchant un logiciel par son nom, on peut avoir la liste des problèmes de sécurité qui y ont été découverts et parfois résolus.

Si ce logiciel a un historique de sécurité parfaitement vierge, ça peut impliquer soit que tout le monde s'en fout, soit que le logiciel est écrit de façon extrêmement rigoureuse.

Si des failles de sécurité ont été découvertes dans le logiciel étudié, il y a plusieurs implications, parfois contradictoires.

1. Ces failles ont été découvertes et corrigées :
 - donc elles n'existent plus, *a priori* ;
 - donc quelqu'un s'est préoccupé de les trouver, et quelqu'un d'autre de les corriger : on peut supposer qu'une attention est donnée à cette question.
2. Ces failles ont existé :
 - le logiciel est peut-être écrit sans que la sécurité soit un souci particulier ;
 - d'autres failles peuvent subsister, non encore découvertes ou pire, non encore publiées.

Afin d'affiner notre intuition par rapport à ce logiciel, il peut être bon de se pencher sur le critère « temps » : par exemple, il n'est pas dramatique que quelques failles aient été découvertes au début du développement d'un logiciel, si aucune n'a été découverte depuis quelques années ; on peut alors mettre ça sur le compte des erreurs de jeunesse. Au contraire, si de nouvelles failles sont découvertes régulièrement, depuis des années, et jusqu'à très récemment, il est fort possible que le logiciel ait encore de nombreux problèmes de sécurité totalement inconnus... ou non publiés.

Pour illustrer le propos, il est possible de comparer l'historique des failles de Claws Mail³ et celui de Thunderbird⁴.

16.2.6 Équipe de développement

Qui a écrit, qui écrit ce logiciel ? Si l'on a réussi à répondre à cette question, divers indices peuvent nous aider à déterminer la confiance qui peut être accordée à l'équipe de développement. Par exemple :


- Les mêmes personnes ont aussi écrit un autre logiciel, que nous utilisons déjà intensivement ; nos impressions sur cet autre logiciel sont tout à fait pertinentes dans le cadre de cette étude.
- Des membres de l'équipe de développement ont des adresses qui finissent par `@debian.org`, et ont donc le droit de modifier les logiciels fournis par Debian GNU/Linux ; si nous utilisons cette distribution, nous accordons déjà, de fait, une certaine confiance à ces personnes.
- Des membres de l'équipe de développement ont des adresses qui finissent par `@google.com`, ce qui montre que Google les paie ; s'il n'y a aucun doute à avoir sur leurs compétences techniques, on peut se demander à quel point leur travail est téléguidé par leur employeur qui, lui, n'est digne d'aucune confiance quant à ses intentions concernant vos données personnelles.


2. L'équipe de sécurité de Debian maintient des informations pour chacun des paquets, visibles sur le *security tracker* [<http://security-tracker.debian.net/tracker/>].

3. <http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=claws+mail>

4. <http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=thunderbird>

16.3 Installer un paquet Debian

 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

 *Durée : 5 minutes, plus le temps de téléchargement et d'installation (quelques secondes à plusieurs heures selon la taille des logiciels à installer et la vitesse de la connexion).*

16.3.1 Ouvrir le gestionnaire de paquets

Une fois que l'on sait quel paquet contient le logiciel que l'on veut utiliser, reste à l'installer. Pour cela, on va utiliser le *Gestionnaire de paquets Synaptic* que l'on peut ouvrir à partir du menu *Applications* → *Outils Système* → *Administration*.

Puisque le gestionnaire de paquets permet de modifier les logiciels installés sur l'ordinateur, un mot de passe est nécessaire pour l'ouvrir.

16.3.2 Recharger la liste des paquets disponibles

Une fois dans le gestionnaire de paquets, commençons par recharger la liste des paquets disponibles en cliquant sur l'icône *Recharger*. Le gestionnaire de paquets télécharge alors les dernières informations sur les paquets disponibles depuis les serveurs de Debian.

16.3.3 Rechercher le paquet à installer

Ensuite, on va trouver le paquet qu'on veut installer. On clique sur l'icône *Rechercher* dans la barre d'outils. Là, si on connaît le nom de ce paquet (par exemple grâce à la section précédente), on l'écrit dans la case *Rechercher*, et on sélectionne *Nom* dans la liste déroulante nommée *Rechercher dans*.

page 116

16.3.4 Sélectionner le paquet à installer

Vient alors la phase d'installation proprement dite du paquet trouvé précédemment. Il y a différentes façons de le faire, selon que l'on souhaite utiliser la version disponible dans les dépôts officiels de sa distribution, ou un paquet provenant d'un autre dépôt, par exemple pour avoir une version plus récente.

Pour installer la version par défaut

Normalement, le paquet désiré se trouve maintenant quelque part dans la liste de paquets. Une fois trouvée la ligne correspondante, on clic-droit dessus, et dans le menu contextuel on choisit *Sélectionner pour installation*.

Si ce paquet dépend d'autres paquets, le gestionnaire de paquets ouvre alors une fenêtre où il demande s'il doit *Prévoir d'effectuer d'autres changements* ? En général, ses propositions sont pertinentes, et on peut accepter en cliquant sur *Ajouter à la sélection*.

Pour installer une version particulière

Parfois, on souhaite installer une version particulière d'un paquet parmi celles disponibles. Par exemple, si on a ajouté des dépôts spécifiques. Au lieu de choisir *Sélectionner pour installation* dans le menu contextuel, il faut sélectionner le paquet désiré d'un clic gauche, puis choisir, dans le menu *Paquet*, de *Forcer la version...* La suite ne change pas.

page 122


16.3.5 Appliquer les modifications


Il est possible de répéter les deux dernières étapes pour installer plusieurs paquets en même temps. Une fois qu'on a préparé cette installation, il ne reste qu'à la lancer en cliquant sur *Appliquer* dans la barre d'outils. Le gestionnaire de paquets ouvre alors une fenêtre *Résumé* où il liste tout ce qu'il va faire. Après avoir jeté un œil pour vérifier qu'on ne s'est pas trompé, on clique sur *Appliquer*.

Le gestionnaire de paquets télécharge alors les paquets depuis Internet, les vérifie, puis les installe. Il peut arriver que le gestionnaire indique que certains paquets n'ont pas pu être vérifiés : cette information n'est pas à prendre à la légère. Dans un tel cas, il vaut mieux annuler le téléchargement, cliquer sur *Recharger* dans le menu principal, et recommencer l'opération de sélection des paquets. Si l'indication apparaît de nouveau, cela peut être le fruit d'une attaque, d'une défaillance technique ou de soucis de configuration. Mais autant s'abstenir d'installer de nouveaux paquets avant d'avoir identifié la source du problème.

Enfin, si tout s'est bien passé, le gestionnaire de paquets affiche une fenêtre comme quoi *Les modifications ont été appliquées* et on peut donc cliquer sur *Fermer*. C'est alors une bonne idée de fermer le gestionnaire de paquets, pour éviter qu'il tombe entre d'autres mains.

16.4 Comment modifier ses dépôts Debian

 Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.

 *Durée : un quart d'heure à une demi-heure.*

Les paquets Debian qui contiennent les programmes se trouvent dans ce qu'on appelle des *dépôts*. Si les dépôts fournis avec Debian contiennent quasiment tous les logiciels dont on peut avoir besoin, il est parfois utile d'installer de nouveaux dépôts, comme *backports.debian.org* qui contient des programmes plus récents que ceux inclus dans la distribution stable de Debian, ou *deb-multimedia.org* qui contient des *codecs* et des logiciels multimédia non-libres, ou interdits dans certains pays, par exemple pour des questions de brevets.



Attention : ajouter un nouveau dépôt Debian sur un ordinateur revient à décider de faire confiance aux gens qui s'en occupent. Si les dépôts de *backports.debian.org* sont maintenus par des membres de Debian, ce n'est pas le cas pour de nombreux autres dépôts. La décision de leur faire confiance ne doit pas se prendre à la légère : si le dépôt en question contient des logiciels malveillants, il serait possible de les installer sur l'ordinateur sans même s'en rendre compte.

page 24

16.4.1 Authenticité du contenu des dépôts

Les dépôts Debian sont signés par des clés GnuPG. Ceci afin de s'assurer que leur contenu n'a pas été altéré par malveillance ou simple problème technique.

Cette section traite rapidement de comment chercher et vérifier une clé GnuPG. Il s'agit de cryptographie asymétrique, technique qui sera traitée plus avant dans le tome 2. On se contentera ici de donner un protocole permettant de vérifier une clé à partir d'une empreinte (ou « *fingerprint* »). On n'apprendra pas à bien utiliser la cryptographie asymétrique.

tome 2 ch. 6

Ce protocole simplifié a des limites : en particulier, on vérifie la clé à partir d'une empreinte (une sorte de somme de contrôle). Toute la confiance que nous allons donner à la clé vient uniquement de cette empreinte. Or vérifier cette empreinte à partir de ce qui est écrit dans ce guide, cela signifie faire fortement confiance à la source à partir de laquelle on l'a obtenu. En lisant ce guide sur Internet, c'est encore pire : on fait, en plus, confiance à sa connexion Internet.

page 41

Encore une fois, tout est affaire de compromis entre utilisabilité et sécurité. Pour obtenir des empreintes en toute confiance, le mieux est de les vérifier en tête-à-tête. Malheureusement, ce n'est généralement pas possible en pratique lorsqu'il s'agit de dépôts Debian. Ce n'est cependant pas une raison pour ne rien vérifier du tout.

Dans le cadre du premier tome de ce guide, qui n'aborde pas les problématiques liées à l'utilisation de réseaux, il n'y a pas de solution vraiment satisfaisante. En attendant le tome 2, qui traitera plus avant de ces questions, le mieux qu'on ait trouvé est d'utiliser :

- des empreintes données dans ce guide, qui ont été vérifiées sur Internet à partir de nombreuses connexions différentes à plusieurs moments différents, mais impliquent de faire confiance à la source de ce guide ;
- si possible, les empreintes qui se trouvent sur d'autres ordinateurs sur lesquels les dépôts en question auraient été installés précédemment si l'on peut y avoir accès, chez des proches par exemple.

Ce protocole est vraiment loin d'être sûr. Il met cependant des bâtons dans les roues de l'éventuelle personne qui souhaiterait nous faire installer des logiciels malveillants.

Quelques empreintes vérifiées par nos soins

Deux des empreintes de dépôts parmi les plus utilisés sont reproduites ci-dessous :

Dépôt	Date	Empreinte
deb-multimedia.org	octobre 1999	1D7F C53F 80F8 52C1 88F4 ED0B 07DC 563D 1F41 B907
deb.torproject.org	septembre 2009	A3C4 F0F9 79CA A22C DBA8 F512 EE8C BC9E 886D DD89

Comparer les empreintes avec celles présentes sur d'autres ordinateurs

Si on peut avoir accès à des ordinateurs sur lesquels les dépôts que l'on souhaite utiliser ont déjà été installés, on pourra recouper les empreintes données dans ce guide avec celles présentes sur ces ordinateurs.

Pour ce faire, sur des ordinateurs variés, ouvrir un *Terminal administrateur* à partir du menu *Applications* → *Accessoires*.

Taper alors :



```
apt-key finger
```

Puis appuyer sur *Entrée*. On obtient alors une liste des clés de dépôts, chacune sous la forme suivante :

```
pub 2048R/886DDD89 2009-09-04 [expire :2014-09-03]
Empreinte de la clé = A3C4 F0F9 79CA A22C DBA8 F512 EE8C BC9E 886D DD89
uid deb.torproject.org archive signing key
sub 2048R/219EC810 2009-09-04 [expire :2012-09-03]
```

C'est la troisième ligne de chaque entrée qui donne le nom du dépôt. Il s'agit dans cette liste de trouver le nom du dépôt qui nous nous intéresse. Dans l'exemple ci-dessus, on a :

```
uid deb.torproject.org archive signing key
```

Il s'agit donc de la clé de *deb.torproject.org*. L'empreinte correspondante se trouve sur la ligne juste au-dessus :

```
Empreinte de la clé = A3C4 F0F9 79CA A22C DBA8 F512 EE8C BC9E 886D DD89
```

Noter alors cette empreinte pour de futures comparaisons.

Récupérer la clé d'un dépôt depuis Internet

Il faut tout d'abord ouvrir *Applications* → *Outils système* → *Préférences* → *Mots de passe et clés*.

- Dans le menu *Distant* choisir *Chercher des clés distantes* ;
- Dans *Chercher des clés contenant*, taper une partie du nom de la clé recherchée ou son identifiant, par exemple « torproject.org » ou « 1F41B907 » (pour deb-multimedia), puis cliquer sur *Chercher* ;

- Une fenêtre *Clés distantes contenant [...] s'ouvre*. Ici on a par exemple « deb.torproject.org archive signing key » qui a pour identifiant **886DDD89** ;
- Cliquer sur cette clé, puis sur le bouton *Importer*.
- On peut alors fermer la fenêtre avec la liste des clés trouvées à distance.

Afin de s'assurer que la clé que l'on vient d'obtenir est bien celle qu'on attend, il s'agit maintenant de vérifier son empreinte :

- Une fois la clé importée, aller dans l'onglet *Affichage* de la fenêtre principale.
- sélectionner l'affichage *Par trousseau*, puis *Tout afficher*
- Dans le nouveau menu, à gauche, sélectionner *Clés GnuPG*
- Sélectionner la clé à vérifier, dans notre exemple « deb.torproject.org archive signing key ».
- Cliquer dessus avec le bouton droit de la souris, et dans le menu contextuel qui apparaît, choisir *Propriétés*.
- Aller dans l'onglet *Détails*.
- Vérifier que l'empreinte correspond à celle relevée par ailleurs pour s'assurer qu'on a la bonne clé.

Si c'est bien le cas, on peut exporter la clé dans un fichier, avant de l'ajouter au logiciel qui s'en servira pour vérifier le contenu des dépôts. Pour cela, fermer la fenêtre avec les propriétés, sélectionner la clé, puis dans *Fichier* cliquer sur *Exporter...* puis l'enregistrer, par exemple dans *Documents*, en acceptant le nom par défaut. On peut fermer *Mots de passe et clés de chiffrement*.

16.4.2 Ajouter un nouveau dépôt

À partir du menu *Applications* → *Outils système* → *Administration* → *Gestionnaire de paquets Synaptic*. Puisque ce logiciel permet de choisir à quels programmes on fait confiance, on est rassuré qu'il nous demande notre mot de passe pour s'ouvrir. Aller dans le menu *Configuration*, puis *Dépôts*.

Configurer l'emplacement du dépôt

Aller dans l'onglet *Other Software*, ce qui signifie « Autre logiciel » (qui ne sont pas fournis officiellement par le projet Debian) et cliquer sur le bouton *Add...* (Ajouter).

Entrer l'adresse du dépôt à ajouter dans la case *Ligne APT* de la boîte de dialogue qui s'ouvre. Par exemple, pour ajouter les *backports* (programmes plus récents que ceux inclus dans la distribution Debian stable) il faut entrer :

```
deb http://ftp.fr.debian.org/debian wheezy-backports main
```

Si l'on souhaite également installer des logiciels non-libres, on peut ajouter *contrib* et *non-free* en plus de *main*. À la place de la ligne précédente, on pourrait plutôt entrer :

```
deb http://ftp.fr.debian.org/debian wheezy-backports main contrib non-free
```

La plupart des dépôts que vous voudrez rajouter ici ne dépendent pas du tout du Projet Debian, par exemple, pour rajouter les dépôts du Projet TOR, il faudrait entrer :

```
deb http://deb.torproject.org/torproject.org wheezy main
```

Une fois que c'est fait, il suffit de cliquer sur *Ajouter une source de mise à jour*.

Pour être sûr que le nouveau dépôt et les paquets qu'il contient sont bien ceux que l'on croit, on doit disposer d'un fichier qui contient la clé avec laquelle sont signées les listes de paquets du dépôt à ajouter, et avoir vérifié cette clé. La télécharger sur un site web et lui faire confiance aveuglément n'est pas une bonne idée.

[tome 2 § 18.2]

Ajouter une nouvelle clé de confiance

Le dépôt contenant les *backports* est devenu un dépôt officiel de Debian avec la sortie de la version *Squeeze* de Debian. La clé de confiance est donc la même que pour le reste des paquets officiels.

Par contre, si on souhaite utiliser le dépôt `deb.torproject.org`, fourni par le projet Tor, il est nécessaire d'ajouter sa clé de confiance. Après suivi la procédure de vérification de la clé, et avoir exporté cette dernière, on procède ainsi :

- Aller dans l'onglet *Authentification* et cliquer sur le bouton *Import Key File...* (importer un fichier de clé) ;
- Sélectionner le fichier où on a précédemment sauvegardé la clé téléchargée — `deb.torproject.org archive signing key.gpg` dans le dossier *Documents* si l'on a suivi les conseils précédents — et cliquer sur *valider*. On pourra ensuite supprimer le fichier en question.

Mettre à jour les paquets disponibles

Il est maintenant possible de retenir les *Sources de mises à jour*. De retour dans le *Gestionnaire de paquets Synaptic*, il faut cliquer sur *Recharger* pour mettre à jour les listes de paquets.

Installer le paquet avec les clés du dépôt

Une fois la clé ajoutée, on a accès au dépôt. Celui-ci fournit généralement un paquet contenant les clés de ce dépôt, et permettant de le mettre aisément à jour. Il est souvent nommé à partir du nom du dépôt, suivi du mot *keyring*. Par exemple, pour `deb.torproject.org`, il s'agit de `deb.torproject.org-keyring`. Il faut donc prendre le temps d'installer ce paquet, s'il est disponible.

[page 120]

Effacer des données « pour de vrai »

On a vu dans la première partie que lorsqu'on efface un fichier, son contenu n'est pas vraiment supprimé. Cependant, il existe des programmes qui permettent d'effacer des fichiers *et leur contenu*, ou du moins qui tentent de le faire, avec les limites expliquées auparavant.

page 32

page 32

17.1 Un peu de théorie

Pour la plupart des prochaines recettes, nous allons utiliser la suite de logiciels *secure-delete*.

17.1.1 La méthode de Gutmann

La documentation¹ du paquet *secure-delete*, inspirée d'une publication de Peter Gutmann publiée en 1996², nous dit (en anglais) :

Le processus d'effacement fonctionne comme suit :

1. *la procédure d'écrasement (en mode sécurisé) remplace le contenu du fichier à 38 reprises. Après chaque passage, le cache du disque est vidé ;*
2. *le fichier est tronqué, de sorte qu'un attaquant ne sache pas quels blocs du disque appartenaient au fichier ;*
3. *le fichier est renommé, de sorte qu'un attaquant ne puisse tirer aucune conclusion sur le contenu du fichier supprimé à partir de son nom ;*
4. *finalement, le fichier est supprimé. [...]*

17.1.2 Le compromis adopté

L'étude de Peter Gutmann porte sur des technologies de disques durs qui n'existent plus de nos jours. Il a depuis ajouté, à la fin de son article, un paragraphe intitulé *Epilogue* qui nous dit, en substance, que pour un disque dur « récent »³, les 38 écritures successives ne sont plus nécessaires : il suffit d'écraser les données quelques fois avec des données aléatoires. Mais mis à part la nature et le nombre de réécritures, le processus décrit précédemment reste tout à fait d'actualité.

De surcroît, le NIST (*National Institute of Standards and Technology*, organisme gouvernemental états-unien définissant les protocoles de sécurité utilisés, entre autres, par les administrations de ce pays) a publié une étude récente⁴ de la NSA, qui semble

1. Fichier README.gz installé sur une Debian dans /usr/share/doc/secure-delete.

2. Peter Gutmann, 1996, *Secure Deletion of Data from Magnetic and Solid-State Memory* [http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html] (en anglais).

3. Utilisant la technologie PRML [<https://fr.wikipedia.org/wiki/PRML>], apparue en 1990 [<http://www.storagereview.com/guide/histFirsts.html>].

4. NIST, 2006, *Guidelines for Media Sanitization* [http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_with-errata.pdf] (en anglais).

conclure que sur les disques durs modernes, les données sont tellement collées les unes aux autres qu'il devient impossible de se livrer à des analyses magnétiques pour retrouver les traces de données effacées ; en effet, la densité des données des disques durs ne cesse de croître, afin d'augmenter leur capacité de stockage.

Par conséquent, nous nous contenterons dans les recettes qui suivent de quelques passages aléatoires, en évoquant tout de même la mise en œuvre de la méthode originale de Gutmann.

[page 51]

Il s'agira une fois de plus de faire le bon compromis, au cas par cas, entre la rapidité et le niveau de protection souhaité, en fonction de la taille des données à écraser, de l'âge du disque dur, et de la confiance qu'on accorde au NIST.

17.1.3 Pour les clés USB et autres mémoires *flash*

Pour les clés USB (ou autre mémoire *flash*), comme les cartes SD, ou disques durs SSD, une étude datant de 2011⁵ a montré que la situation était réellement problématique.

Cette étude démontre qu'il est impossible d'avoir la garantie d'avoir recouvert tout le contenu d'un fichier donné, quel que soit le nombre de réécritures. Même si cela rend inaccessibles les données en branchant simplement la clé, elles sont toujours visibles pour quiconque regarderait directement dans les puces de mémoire *flash*.

La seule méthode qui a fonctionné de façon systématique était de réécrire plusieurs fois l'*intégralité* de la clé USB. Dans la plupart des cas, deux passages ont suffi, mais sur certains modèles, vingt réécritures ont été nécessaires avant que les données ne disparaissent pour de bon.

[page 137]

Partant de ces constats, la réponse préventive semble être de chiffrer systématiquement les clés USB, opération rendant vraiment plus difficile d'extraire des informations directement depuis les puces de mémoire *flash*. Et pour nettoyer a posteriori, l'écrasement entier, malgré ses limites, protège tout de même contre les attaques purement logicielles.

17.1.4 D'autres limites de l'effacement « sécurisé »



Il peut encore rester des informations sur le fichier permettant de le retrouver, notamment si l'on utilise un système de fichiers journalisé comme *ext3*, *ext4*, ReiserFS, XFS, JFS, NTFS, un système d'écriture, de compression ou de sauvegarde, sur disque (exemple : RAID) ou via un réseau. Voir à ce sujet la première partie.

[page 33]

17.2 Sur d'autres systèmes

[page 29]

On a vu qu'il est illusoire, si l'on utilise un système d'exploitation propriétaire, de rechercher une réelle intimité. Bien qu'il existe des logiciels supposés effacer des fichiers avec leur contenu sous Windows et Mac OS X, il est donc bien plus difficile de leur faire confiance.


17.3 Allons-y


On peut effacer le contenu :

- de fichiers individuels, voir page ci-contre ;
- de tout un périphérique, voir page suivante ;
- de fichiers déjà supprimés, voir page 135.


5. Michael Wei et Al, 2011, *Reliably Erasing Data From Flash-Based Solid State Drives* [https://www.usenix.org/legacy/events/fast11/tech/full_papers/Wei.pdf] (en anglais).

17.4 Supprimer des fichiers... et leur contenu

 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

 *Durée : 5 minutes de préparation, puis quelques secondes à plusieurs heures d'attente en fonction de la taille du fichier à effacer et de la méthode utilisée.*

Voici donc la méthode à suivre pour se débarrasser de fichiers, en prenant soin de rendre illisible ce qu'ils contenaient.

 **Attention!** Après avoir recouvert le contenu de fichiers sur une clé USB (ou tout autre support de stockage utilisant de la mémoire flash comme une carte SD ou disque dur SSD) il y a de fortes chances qu'il se trouve encore inscrit dans une région inaccessible de la clé!

17.4.1 Installer les logiciels nécessaires

Si ce n'est pas déjà fait, il nous faut installer `nautilus-wipe`. Ce paquet est présent par défaut dans *Tails*. page 120

17.4.2 Supprimer des fichiers et leur contenu à partir du navigateur de fichiers

Dans *Tails*

Afin de supprimer des fichiers et leur contenu en utilisant *Tails*, consulter la documentation en cliquant sur l'icône *Documentation de Tails* se trouvant sur le bureau. Dans le menu à droite, cliquer sur *Documentation*. Dans l'index qui s'ouvre, chercher la section *Chiffrement et vie privée* et cliquer sur la page *Effacer des fichiers de façon sécurisée et nettoyer l'espace disque avec Nautilus Wipe*.

Avec une Debian chiffrée

Afin de supprimer des fichiers et leur contenu depuis le navigateur de fichiers, naviguer jusqu'au fichier, faire un clic-droit sur celui-ci et sélectionner *Écraser*. Une fenêtre s'ouvre nous demandant de confirmer la suppression, et proposant également quelques *Options*.

Nous pouvons choisir le nombre de passes effectuées afin de recouvrir les données de notre périphérique ainsi que quelques options de comportement lors de l'effacement des données. Les options par défaut sont suffisantes pour les disques durs actuels.

Cliquer ensuite sur *Écraser*. Une fois l'effacement terminée, une fenêtre *L'écrasement a réussi* s'ouvre, précisant que *Le(s) élément(s) ont été écrasé(s) avec succès..*

17.5 Effacer « pour de vrai » tout un disque

Avant de se débarrasser d'un disque dur, de le recycler, de réinstaller un système propre, ou encore d'envoyer un ordinateur en panne au Service Après Vente, il peut être judicieux de mettre des bâtons dans les roues des gens qui voudraient récupérer les données qu'il contenait. Pour cela, la meilleure solution est encore de les remplacer par du charabia. page 57

Avant d'utiliser cette recette, il faut réfléchir à deux fois et sauvegarder soigneusement les données à conserver. Si elle est bien appliquée, elle rend en effet les données très difficiles à récupérer, même en analysant le disque dans un laboratoire. page 143

Nous verrons d'abord comment effacer tout le contenu d'un disque, puis comment rendre le contenu d'une partition chiffrée inaccessible rapidement.

17.6 Effacer tout le contenu d'un disque

🔄 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

🕒 *Durée : 5 minutes de préparation, puis plusieurs heures d'attente en fonction de la taille du disque.*

Pour effacer un volume complet (disque ou partition), on va utiliser la commande `shred` de façon à ce qu'elle recouvre la totalité des données trois fois avec des données aléatoires. Cette commande permet donc, en plus de l'effacement des fichiers, de recouvrir l'espace effacé de telle manière qu'il devient quasiment impossible de retrouver ce qu'il contenait auparavant.

Pour recouvrir le contenu d'un disque, il est nécessaire de ne pas être en train de l'utiliser... s'il contient le système d'exploitation habituellement utilisé, il faut donc mettre le disque dur dans un autre ordinateur ou utiliser un système *live*. `shred` étant un outil standard, n'importe quel système *live* devrait faire l'affaire.

La commande est très simple. Elle exige seulement de connaître l'emplacement du périphérique (son chemin) que l'on veut effacer, puis de faire preuve de patience car le processus prend plusieurs heures.

17.6.1 Trouver le chemin du périphérique

Avant tout, il faut savoir repérer sans se tromper le chemin utilisé par le système d'exploitation pour désigner le support de stockage qu'on veut effacer.

Si l'on souhaite effacer un disque interne, commencer par débrancher tous les disques durs externes, clés USB, lecteurs de cartes mémoire ou autre périphérique de stockage branchés sur l'ordinateur. D'une part, cela évitera de les effacer par erreur ; d'autre part, cela rendra la recherche du disque interne plus facile.

Bien sûr, il ne faut pas faire cela si c'est justement le contenu d'un disque externe que l'on souhaite rendre inaccessible.

Ouvrir l'Utilitaire de disque

Pour trouver le chemin du périphérique, une méthode simple consiste à utiliser l'*Utilitaire de disque* que l'on démarre par le menu *Applications* → *Accessoires*.

Chercher le chemin du périphérique

La partie située à gauche indique la liste des disques durs connus du système. On peut cliquer sur l'un d'entre eux afin de voir plus d'informations apparaître sur la partie droite. Les icônes, la taille indiquée ainsi que le nom des disques devraient permettre d'identifier celui que l'on cherche.

Si cela ne suffit pas, il est possible de jeter un œil à l'organisation des partitions, en regardant le tableau qui apparaît dans la partie droite :

- si le disque à effacer contenait un système GNU/Linux non chiffré, il doit y avoir au moins deux partitions, l'une avec un système de fichiers *swap*, l'autre en général *ext3* ;
- si le disque à effacer contenait un système GNU/Linux chiffré, il doit y avoir au moins deux partitions, l'une avec un système de fichiers *ext2*, l'autre en général *Chiffré* ou *Inconnu* ;
- si le disque à effacer contenait un système Windows, il doit y avoir une ou plusieurs partitions notées *ntfs* ou *fat32*.

Par ailleurs, le périphérique correspondant au disque interne est généralement le premier de la liste.

Une fois le disque trouvé et sélectionné, on pourra lire le chemin du disque dans la partie à droite, sous l'intitulé *Disque*, à côté de l'étiquette *Périphérique*.

Le chemin du périphérique commence par `/dev/` suivi de trois lettres, les deux premières étant `sd` ou `hd` : par exemple, `/dev/sdx`. Noter le chemin quelque part : il faudra l'écrire tout à l'heure à la place de `LE_PÉRIPHÉRIQUE`.



Attention! Ce chemin n'est pas nécessairement toujours le même. Il vaut mieux recommencer cette courte procédure après avoir redémarré l'ordinateur, branché ou débranché une clé USB ou un disque dur. Cela évitera les mauvaises surprises... comme perdre le contenu d'un *autre* disque dur.

17.6.2 Lancer la commande *shred*

Ouvrir un *Terminal administrateur* à partir du menu *Applications* → *Accessoires*.

[page 85]

Saisir la commande suivante en veillant à remplacer `LE_PÉRIPHÉRIQUE` par le chemin de périphérique déterminé précédemment :



```
shred -n 3 -v LE_PÉRIPHÉRIQUE
```

Si l'on préfère utiliser la méthode originale de Gutmann (plus longue, et peut-être plus sûre), il faut remplacer `-n 3` par `-n 25` dans la ligne de commande.

Une fois la commande tapée et vérifiée, appuyer sur la touche *Entrée*. La commande `shred` va alors écrire dans le terminal ce qu'elle fait (ainsi qu'on lui a demandé de le faire en ajoutant à la commande `shred` l'option `-v`, qui signifie, dans le cadre de *cette* commande, que l'ordinateur doit être « verbeux » — c'est-à-dire « bavard ») :

```
shred :/dev/sdb :pass 1/3 (random)...
shred :/dev/sdb :pass 2/3 (random)...
shred :/dev/sdb :pass 3/3 (random)...
```

À la fin de la procédure, le terminal affiche à nouveau le signe `#`, qui symbolise l'invite de commande. On peut alors fermer le terminal.


17.6.3 Réutiliser le disque


Attention, cette méthode efface non seulement les données d'un volume complet mais, à la fin de l'opération, le disque n'a plus ni table de partitions, ni système de fichiers. Pour le réutiliser, il est nécessaire de créer entièrement au moins une nouvelle partition et son système de fichiers, avec l'*Utilitaire de disque* par exemple.

[page 16]

[page 16]

17.7 Effacer le contenu d'une partition chiffrée LUKS

 Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.

 Durée : 10 minutes environ.

Il est extrêmement rapide de rendre inaccessible le contenu d'une partition LUKS, le format de stockage standard des clés de disques chiffrés sous GNU/Linux.

page 37

Certains logiciels de chiffrement d'un disque complet ont en effet la capacité de détruire la clé de chiffrement, rendant ainsi le contenu chiffré incompréhensible. Vu que la clé contient une part minuscule d'informations et peut être détruite presque instantanément, cette méthode est une alternative bien plus rapide à l'écrasement de l'ensemble des données.

page 130

Ceci dit, cette option n'est réalisable que si le disque dur a déjà été chiffré. Si les données confidentielles contenues sur le disque ne sont pas déjà chiffrées, il est nécessaire d'effacer le disque entier, comme expliqué précédemment, avant de pouvoir s'en débarrasser ou le réutiliser en toute tranquillité.



Attention! Sur une clé USB (ou tout autre support de stockage utilisant de la mémoire *flash*), cette méthode ne permet pas de garantir que les données ainsi recouvertes soient réellement rendues inaccessibles. Il est donc nettement plus sûr de recouvrir plusieurs fois l'intégralité des données de la clé.

page 130

17.7.1 Repérer la partition en question

Comme dans le cas précédent, si l'on souhaite effacer un disque interne, commencer par débrancher tous les disques durs externes, clés USB, lecteurs de cartes mémoire ou autre périphérique de stockage branchés sur l'ordinateur. D'une part, cela évitera de les effacer par erreur ; d'autre part, cela rendra la recherche du disque interne plus facile.

Bien sûr, il ne faut pas faire cela si c'est justement le contenu d'un disque externe que l'on souhaite rendre inaccessible.

Ouvrir l'Utilitaire de disque

On va s'aider de l'*Utilitaire de disque*, que l'on ouvre à partir du menu *Applications* → *Accessoires*.

Chercher le disque en question

La partie située à gauche indique la liste des disques durs connus du système. Les icônes, la taille indiquée ainsi que le nom des disques devraient permettre d'identifier celui que l'on cherche. On peut cliquer sur l'un d'entre eux afin de voir plus d'informations apparaître sur la partie droite.

Le premier périphérique que l'*Utilitaire de disque* affiche dans cette liste est généralement le disque dur interne.

Chercher le chemin de la partition

Lorsqu'un disque est sélectionné dans la liste de gauche, plus d'informations à son sujet apparaissent dans la partie droite de la fenêtre. On s'intéressera en particulier au schéma des *Volumes*, ou partitions.

Normalement, les partitions chiffrées sont indiquées dans la partie *Volumes* avec comme indication *Chiffré...* mais ce n'est pas toujours le cas : l'*Utilitaire de disque*

peut aussi indiquer que le type de partition est *inconnu*, ou parfois indiquer un type plus courant (*ext3*, *NTFS*).

Une fois la partition chiffrée à effacer repérée sur le schéma, cliquer dessus. Son chemin apparaît alors sous le schéma à droite, à côté de l'étiquette *Périphérique*. C'est ce chemin que nous allons noter. Nous l'appellerons `LE_PÉRIPHÉRIQUE_CHIFFRÉ`. Ce doit être quelque chose comme `/dev/sdx9`.

17.7.2 Ouvrir un terminal administrateur

À partir du menu *Applications* → *Accessoires*, ouvrir un *Terminal administrateur*.

page 85

17.7.3 Vérifier le premier repérage et récupérer la taille de l'en-tête LUKS

Dans le terminal, la commande `cryptsetup luksDump` donne plein d'informations sur l'en-tête LUKS, dont sa taille sur le disque (en secteurs de 512 octets). Taper donc, en remplaçant `LE_PÉRIPHÉRIQUE_CHIFFRÉ` par la valeur déterminée ci-dessus :



```
cryptsetup luksDump LE_PÉRIPHÉRIQUE_CHIFFRÉ
```

Dans le cas où on se serait trompé de périphérique, le terminal ne renvoie soit aucune réponse, soit :

```
LE_PÉRIPHÉRIQUE_CHIFFRÉ n'est pas un périphérique LUKS valide.
```

Si l'on ne s'est pas trompé, on doit plutôt se voir répondre quelque chose comme :

```
LUKS header information for /dev/sdx2

Version :      1
Cipher name :  aes
Cipher mode :  cbc-essiv sha256
Hash spec :    sha1
Payload offset :4096
MK bits :      256
MK digest :    a4 79 85 49 1f 3f 71 e5 1e c6 07 14 88 0c 02 27
                59 80 25 58
MK salt :      b7 b1 2a 5d 6d c5 b5 d2 06 55 a3 85 5d 07 af 9b
                c9 03 46 c6 e6 2f 29 1a 9d b7 58 05 44 cc 68 f9
MK iterations : 54520
UUID :         d73cbb8a-058f-469e-935a-7f71debd8193

Key Slot 0 : ENABLED
  Iterations :      217000
  Salt :            ec 1e 63 b7 13 fb 20 21 18 5d 86 44 42 d0
                   f2 af 52 a4 74 54 22 3f d8 0b ad 69 8c 46
                   f2 d3 79 4d
  Key material offset 8
  AF stripes :      4000
```

On va avoir besoin de la taille de l'en-tête (en secteurs), écrite sur la ligne `Payload offset` : la noter quelque part. On l'utilisera plus loin sous le nom d'`OFFSET`.

17.7.4 Recouvrir l'en-tête LUKS de données aléatoires

Comme dans la recette précédente, on va utiliser la commande `shred` pour écraser les données, mais cette fois on écrasera uniquement l'en-tête LUKS (cet en-tête contient la clé qui permet de déchiffrer le reste des données). Cela ira donc beaucoup plus vite.

Dans le terminal administrateur, saisir la commande suivante en prenant bien soin de remplacer `OFFSET` et `LE_PÉRIPHÉRIQUE_CHIFFRÉ` par les valeurs qu'on a trouvées :



```
shred -n 3 -s $((OFFSET * 512)) -v LE_PÉRIPHÉRIQUE_CHIFFRÉ
```

Appuyer alors sur *Entrée*.

page 85

Note : l'option `-s` utilisée ici sert, dans le cadre de *cette* commande, à indiquer la taille (*size*) de l'espace qui doit être effacé de manière sécurisée.

Une fois que le terminal rend la main, les données chiffrées devraient être illisibles. Pour s'en assurer, il est possible de chercher un en-tête LUKS qui n'aurait pas été bien effacé en tapant à nouveau :



```
cryptsetup luksDump LE_PÉRIPHÉRIQUE_CHIFFRÉ
```

Si l'en-tête a bien été effacé, le terminal renvoie soit aucune réponse, soit :

```
LE_PÉRIPHÉRIQUE_CHIFFRÉ n'est pas un périphérique LUKS valide.
```

page 130

Enfin il est possible, voire même conseillé, d'effacer quand même l'ensemble de la partition, en suivant [la recette précédente](#).

17.8 Rendre irrécupérables des données déjà supprimées

🔄 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

🕒 *Durée : 5 minutes de préparation, puis de plusieurs minutes à plusieurs heures d'attente, selon la taille du disque à nettoyer et selon la méthode utilisée.*

Lorsque des fichiers ont déjà été effacés sans précautions particulières, les données qu'ils contenaient se trouvent toujours sur le disque. L'objectif de cette recette est de recouvrir les données qui subsisteraient, en écrasant l'espace libre d'un disque dur.

⚠️ **Attention!** Comme les autres façons d'effacer un fichier « pour de vrai », cela ne marche pas avec certains systèmes de fichiers « intelligents » qui, pour être plus efficaces, ne vont pas montrer tout l'espace libre au logiciel chargé d'y recouvrir les traces. Voir à ce sujet la première partie. Il ne faut pas non plus faire confiance à cette méthode pour une clé USB, les cartes SD ou disques durs SSD et préférer recouvrir plusieurs fois l'intégralité des données qu'elle contient.

page 33
page 130

Dans *Tails*

Le paquet `nautilus-wipe` est déjà installé par défaut dans *Tails*. Il nous suffit donc de consulter la documentation, en cliquant sur l'icône *Documentation de Tails* se trouvant sur bureau.

Dans le menu à droite, cliquer sur *Documentation*. Puis, dans l'index qui s'ouvre, chercher la section *Chiffrement et vie privée* et cliquer sur la page *Effacer des fichiers de façon sécurisée et nettoyer l'espace disque avec Nautilus Wipe*.

Avec une Debian chiffrée

Si ce n'est pas déjà fait, il nous faut installer le paquet, voir page 120 `nautilus-wipe`.

Il nous faut ensuite ouvrir un navigateur de fichiers, puis naviguer jusqu'au disque que l'on veut nettoyer. Effectuez ensuite un clic-droit dans la partie droite du navigateur de fichiers et sélectionnez *Écraser l'espace disque disponible*. Une fenêtre s'ouvre nous demandant de confirmer la suppression de l'espace disque disponible, et proposant également quelques *Options*.

Nous pouvons choisir le nombre de passes effectuées afin de recouvrir les données de notre périphérique, ainsi que quelques options de comportement lors de l'effacement des données. Les options par défaut sont suffisantes pour les disques durs actuels.

Cliquer ensuite sur *Écraser l'espace disque disponible*. L'effacement peut prendre du temps. Remarquons qu'un fichier appelé `oooooooo.ooo` est créé dans le dossier. *Nautilus Wipe* va en augmenter la taille autant que possible, afin d'utiliser tout l'espace libre disponible, puis l'écrasera de manière sécurisée. Une fois l'effacement terminé, une fenêtre *L'écrasement a réussi* s'ouvre, précisant que *L'espace disque disponible sur la partition ou le périphérique « ... » a été écrasé avec succès*.

Partitionner et chiffrer un disque dur

Nous allons maintenant aborder le chiffrement d'un périphérique, afin d'y stocker des données de manière chiffrée.

Une fois un disque dur chiffré, les données qu'il contient ne sont accessibles que lorsqu'on a tapé une phrase de passe permettant de le déchiffrer. Pour plus d'informations là-dessus, consultez la [partie sur la cryptographie](#).

page 37

Une fois la phrase de passe saisie, le système a accès aux données du disque dur en question, il ne faut donc pas taper cette phrase de passe n'importe où, mais seulement sur les ordinateurs et les systèmes dans lesquels on a [suffisamment confiance](#).

page 51

En effet, non seulement ceux-ci auront accès aux données déchiffrées, mais des traces de la présence du disque dur seront également gardées sur l'ordinateur. C'est pourquoi nous vous conseillons de l'utiliser sur un [système GNU/Linux chiffré](#) ou un [système *live* amnésique](#).

page 19

page 105

page 99

Il peut s'agir d'un disque dur externe, d'une clé USB, d'une carte SD ou encore d'une partie seulement d'un de ces périphériques. On peut en effet découper un disque dur ou une clé USB en plusieurs morceaux indépendants, qu'on appelle des [partitions](#).

page 16

Ci-dessous, on parlera de disque dur, sachant que, sauf mention contraire, le terme vaut aussi bien pour un disque dur externe, une clé USB, ou une carte SD.

Si on veut avoir un endroit sur le disque dur où mettre des données qui ne seront pas confidentielles, mais auxquelles on pourra accéder sur des ordinateurs non dignes de confiance, il est possible de découper le disque dur en deux partitions :

- une partition non chiffrée, où l'on ne met que des données non confidentielles, comme de la musique, que l'on peut utiliser depuis tous les ordinateurs sans taper la phrase de passe ;
- une partition chiffrée, avec les données confidentielles, qu'on n'ouvre que sur les ordinateurs auxquels on fait confiance.

18.1 Chiffrer un disque dur avec LUKS et dm-crypt

On va expliquer comment chiffrer un disque avec les méthodes standards sous GNU/Linux, appelées `dm-crypt` et `LUKS`. Ce système est maintenant bien intégré avec les environnements de bureau, et la plupart des opérations sont donc possibles sans avoir besoin d'outils particuliers.

18.2 D'autres logiciels que l'on déconseille

page 29

Il existe d'autres logiciels de chiffrement comme FileVault¹, qui est intégré dans Mac OS X — mais il s'agit d'un logiciel propriétaire — ou TrueCrypt — mais on a moins de raisons de lui faire confiance que le chiffrement standard de GNU/Linux, car il n'est plus mis à jour depuis mai 2014 et ce n'était pas vraiment un logiciel libre². De plus, si l'on utilise un logiciel, même libre, sur un système d'exploitation propriétaire, on fait implicitement confiance à ce dernier car il a forcément accès aux données déchiffrées.

page 15

18.3 En pratique

Si le disque dur a déjà servi, il peut être nécessaire de commencer par recouvrir ses données, voir page 127.

Si le disque à chiffrer ne dispose pas d'espace libre, le formater, voir page ci-contre.

Ensuite, si l'on souhaite chiffrer une partie seulement du disque dur, il faut créer une partition en clair, voir page 140.


À la suite de quoi il ne reste plus qu'à l'initialiser pour contenir des données chiffrées, voir page 140.


Le voilà enfin prêt à être utilisé, voir page 141.

1. La dernière analyse indépendante de FileVault [<http://crypto.nsa.org/vilefault/23C3-VileFault.pdf>] date de 2006. En plus d'être sensible aux mêmes attaques que d'autres systèmes, FileVault a quelques faiblesses qu'il faut préciser : ce système ne permettant de chiffrer que le répertoire personnel, des traces seront écrites [page 19] en clair sur le reste du disque dur ; la phrase de passe de chiffrement est identique au mot de passe de la session, généralement faible ; le fait d'enregistrer un « mot de passe principal » ouvre un nouveau champ d'attaques ; la clé de chiffrement sera écrite sur le disque dur si *Utiliser la mémoire virtuelle sécurisée* n'a pas été choisi, ou si un ordinateur mis en veille vide sa batterie. Néanmoins, en gardant en tête que cela offre un niveau de protection limité, cela vaut tout de même la peine d'activer FileVault sur un ordinateur avec Mac OS X.

2. TrueCrypt, dont le développement a été interrompu [<http://truecrypt.sourceforge.net/>] en mai 2014, était distribué sous une licence particulière, la « *TrueCrypt License* » : le développement n'était pas ouvert, et seules les sources de la dernière version sont disponibles, ce qui rend plus difficile la vérification des modifications apportées. De plus, le logiciel n'est pas considéré comme libre par nombre de distributions GNU/Linux, notamment Debian, et ne correspond pas à la définition de l'*open source* de l'Open Source Initiative [<http://www.opensource.org/docs/osd>].

18.4 Préparer un disque à chiffrer

 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

 *Durée : environ 10 minutes.*

Ci-dessous, on parlera toujours de disque dur, sachant que ça vaut aussi bien pour un disque dur externe que pour une clé USB, sauf si on précise le contraire.

La procédure que l'on explique ici implique d'effacer toutes les données qui se trouvent sur le disque³. Si l'on a déjà de l'espace non partitionné sur son disque, on peut directement passer à l'étape de chiffrement.

[page suivante]

18.4.1 Installer les paquets nécessaires

Pour chiffrer notre disque dur, on a besoin d'avoir installé les paquets `secure-delete`, `dosfstools` et `cryptsetup`. Si l'on utilise Tails, ces paquets sont déjà installés.

[page 120]

18.4.2 Formater le disque dur avec l'Utilitaire de disque

Aller dans *Applications* → *Accessoires* → *Utilitaire de disque*.

Une fenêtre s'ouvre. La partie de gauche liste les disques connus du système. La partie de droite permet d'effectuer des actions.

Choisir le périphérique

À gauche, dans la section *Disques périphériques*, il y a la liste des disques. Si l'ordinateur utilisé contient un système chiffré, il y a aussi les volumes chiffrés de notre système.

Les icônes, la taille indiquée ainsi que le nom des disques devraient permettre d'identifier celui que l'on cherche.

Une fois le disque repéré, le sélectionner dans la liste.

Démonter les volumes

Si le volume est monté, un bouton *Démonter le volume* sera accessible dans le menu de droite, sous l'onglet *Volumes*. Cliquer sur ce bouton afin de démonter le volume. Si ce disque contient plusieurs volumes, les démonter tous, un par un.

Reformater le disque



Attention! Formater un disque dur revient à supprimer tous les fichiers qui s'y trouvent.

Dans le menu de droite, sous l'onglet *Disque*, cliquer sur *Formater le disque*, puis choisir, comme *Schéma*, *Master Boot Record* et cliquer sur *Formater*. L'utilitaire de disque demande si l'on veut vraiment formater le périphérique. C'est le moment de vérifier que l'on a choisi le bon périphérique avant de faire une bêtise. Si c'est bien le cas, confirmer en cliquant sur *Formater*.

³. On pourrait également utiliser le logiciel GParted. Plus difficile à utiliser que l'*Utilitaire de disque*, ce dernier à l'avantage de savoir *redimensionner* une partition déjà existante tout en gardant les fichiers qui s'y trouvent.

18.5 Créer une partition non chiffrée

🔄 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

🕒 *Durée : 2 minutes.*

On ouvrira la partition chiffrée qui contiendra nos données confidentielles uniquement sur les ordinateurs auxquels on fait confiance.

Si on le souhaite, c'est le moment de créer une partition non chiffrée où l'on met des données qui ne sont pas confidentielles, et que l'on peut utiliser depuis tous les ordinateurs sans avoir à taper la phrase de passe.

plus bas

Si l'on désire chiffrer le disque dur en entier, on peut directement passer à l'étape suivante.

Toujours avec l'*Utilitaire de disque* et le disque dur sélectionné, dans la partie droite cliquer sur la zone *Libre* du schéma des *Volumes*. En-dessous, cliquer ensuite sur *Créer une partition*.

Placer le curseur *Taille* à la taille voulue pour la partition non chiffrée. L'espace laissé libre nous servira pour la partition chiffrée. Dans *Type*, choisir *FAT*. On peut aussi choisir un nom pour la partition. Une fois cela fait, cliquer sur *Créer*.

18.6 Créer une partition chiffrée

🔄 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

🕒 *Durée : 10 minutes + quelques minutes à plusieurs heures pour remplir l'espace libre, selon la taille de la partition.*

18.6.1 Créer la partition chiffrée

Sur le schéma des *Volumes*, cliquer sur *Libre*. En-dessous, cliquer sur *Créer une partition* : une fenêtre s'ouvre.

Dans la section *Type*, choisir *FAT*. Entrer un nom pour la partition (en lettres, sans espaces ni caractères spéciaux, sinon ça risque fort de ne pas marcher) et cocher la case *Chiffrer le périphérique correspondant*. Valider en cliquant sur *Créer*.

page 91

Une fenêtre s'ouvre alors, qui demande la phrase de passe. Il faut en choisir une bonne, et la taper dans les deux cases correspondantes, avant de valider en cliquant sur *Créer*.

18.6.2 Remplir la partition de données aléatoires

Pour finir, on va remplir l'espace vide du disque dur de données aléatoires. Cela permet de cacher l'endroit où vont se trouver nos propres données, et complique donc la vie des personnes qui voudraient tenter de les déchiffrer.

Sur le schéma des *Volumes*, cliquer sur la partition *FAT* en-dessous de *Chiffré*, puis, à gauche sous le schéma, cliquer sur *Monter le volume*.

Ouvrir ensuite le dossier en le sélectionnant dans la liste située en-dessous de *Poste de travail* dans l'onglet *Raccourcis* du tableau de bord. Une fois le dossier correspondant à la clé ouverte on va suivre l'outil servant à rendre irrécupérables des données déjà

page 135

supprimées.

Le processus dure de quelques minutes à quelques heures, selon la taille du disque dur et sa vitesse (par exemple, 2 heures pour une clé USB de 4 Go).

18.6.3 Débrancher *proprement* le disque dur

Retourner dans l'*Utilitaire de disque*, cliquer sur *Démonter le volume*. Attendre un peu, puis sur le schéma des volumes, cliquer sur le volume *Chiffré* au-dessus du volume *FAT*. Cliquer alors sur *Verrouiller le volume* sous le schéma à droite (s'il y a un message d'erreur, ce n'est pas très grave), puis sur *Déconnexion en toute sécurité*, au-dessus du schéma à droite. Débrancher ensuite physiquement le disque externe de l'ordinateur. On peut désormais fermer l'*Utilitaire de disque*.

Le disque dur chiffré est maintenant utilisable.

18.7 Utiliser un disque dur chiffré

🔄 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

🕒 *Durée : 2 minutes, quelques heures... ou jamais, selon notre capacité à retenir la phrase de passe.*

Afin de permettre au système d'accéder aux données qui se trouvent sur un disque chiffré, il est heureusement nécessaire d'indiquer la phrase de passe. Une opération plus ou moins simple selon les environnements...

18.7.1 Avec Debian (ou autre GNU/Linux)

Sur un système GNU/Linux avec un environnement de bureau configuré pour monter automatiquement les médias externes, une fenêtre apparaît pour demander la phrase de passe lorsqu'on branche un disque externe contenant des données chiffrées.

Si ce n'est pas le cas, elle apparaîtra quand on demandera au système de monter la partition, par exemple à partir du *Poste de travail*.

Pour fermer la partition chiffrée, il suffit de démonter le disque dur comme on le fait habituellement.

18.7.2 Avec d'autres systèmes

Nous ne connaissons pas de moyen simple d'accéder à la partition chiffrée du disque dur ni sous Windows, ni sous Mac OS X. Même si des solutions peuvent exister⁴, il est bon de rappeler qu'il s'agit de systèmes d'exploitation propriétaires, en lesquels il n'y a aucune raison d'avoir confiance.

[page 29]

Alors le mieux à faire, pour mettre sur le disque dur des données auxquelles on veut accéder sur des ordinateurs en lesquels on n'a pas confiance, c'est de mettre une deuxième partition, non chiffrée, sur le disque dur, comme expliqué précédemment.

[page précédente]

4. Pour les anciennes versions de Windows (jusqu'à Vista), il était possible d'utiliser FreeOTFE (<http://sourceforge.net/projects/freeotfe.mirror/>).

Sauvegarder des données

Réaliser des sauvegardes est une opération relativement simple dans son principe : faire une copie des fichiers qu'on ne voudrait pas perdre, sur un autre support de stockage que celui où se trouvent les données.

Bien entendu, si on prend le soin de mettre nos données de travail sur des disques durs ou des clés USB chiffrés, il est nécessaire que ces copies soient chiffrées, elles aussi.

Deux autres points à ne pas négliger pour mettre en place une bonne *politique de sauvegardes* :

- définir une méthode pour effectuer **régulièrement** ses sauvegardes,
- tester de temps à autre si les sauvegardes sont toujours bien lisibles.

Ce dernier aspect est vraiment à ne pas négliger. Perdre les données originales est souvent pénible. S'apercevoir ensuite que les sauvegardes ne permettent pas de *restaurer* ce qu'on a perdu transforme la situation en catastrophe.

Dans le même ordre d'idée, cela paraît également une bonne idée de ne pas stocker les sauvegardes au même endroit que les données originales. Sinon, on risque que les deux soient perdues ou détruites simultanément...

19.1 Gestionnaire de fichiers et stockage chiffré

Réaliser des sauvegardes est avant tout une question de rigueur et de discipline. Dans les cas simples, on peut se passer de logiciels spécialement prévus pour réaliser des sauvegardes, et se contenter simplement d'effectuer des copies avec le gestionnaire de fichiers.

19.1.1 Effectuer les sauvegardes

🔄 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

🕒 *Durée : pour la première fois, le temps de chiffrer le support de stockage et de décider des fichiers à sauvegarder ; et ensuite cela dépend de la quantité de données à sauvegarder.*


Le chiffrement de nos sauvegardes sera assuré par le chiffrement du support de stockage externe (clé USB ou disque dur). page 137

Pour effectuer les copies avec régularité et sans trop y passer de temps, il est recommandé :

- d'avoir quelque part une liste des fichiers et dossiers à sauvegarder ;
- de se fabriquer un petit calendrier des jours ou semaines où l'on fera ses sauvegardes, avec des cases que l'on cochera après les avoir faites.

Une bonne pratique consiste à créer un dossier avec la date de la sauvegarde pour y copier les données. Cela permet de garder facilement plusieurs sauvegardes si on le souhaite, et de supprimer tout aussi facilement les sauvegardes précédentes.


19.1.2 Restaurer une sauvegarde


 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

 *Durée : selon la quantité de données à restaurer.*

En cas de perte des données originales, la restauration se fait aussi simplement que la sauvegarde : en effectuant des copies dans l'autre sens.

19.1.3 S'assurer que les sauvegardes sont toujours lisibles

 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

 *Durée : environ 5 minutes + attendre que la vérification se fasse.*

Si l'on a effectué nos sauvegardes sur un support de stockage externe, il faut commencer par le brancher sur l'ordinateur.

La méthode évidente pour s'assurer que les sauvegardes sont toujours lisibles est sans doute de simuler une restauration. Procéder ainsi a un inconvénient... de taille : il faut avoir assez d'espace libre à notre disposition pour recopier l'ensemble des données sauvegardées vers un dossier temporaire que l'on supprime ensuite.

Voici une autre méthode, peut-être moins facile à mettre en œuvre, mais qui n'a pas cette contrainte. Elle nécessite d'utiliser un *Terminal*.

page 85

On va commencer la commande en tapant (**sans** faire *Entrée*) :

\$>

```
find
```

Ajouter ensuite un espace. Puis il faut indiquer le dossier contenant les sauvegardes, ce que l'on va faire avec la souris, en attrapant l'icône du dossier et en l'amenant sur le terminal. Après avoir relâché le bouton, ce qui est affiché doit ressembler à :

\$>

```
find '/media/externe/sauvegardes'
```

Il faut ensuite taper la fin de la commande pour que le tout ressemble à :

\$>

```
find '/media/externe/sauvegardes' -type f -print0 | xargs -0 cat > /dev/null
```

La lecture se lance dès qu'on a appuyé sur *Entrée*. La ligne suivante devrait rester vide jusqu'à la fin de l'opération.

Après de la patience et le retour du \$ de l'invite de commande, on peut fermer le terminal.

Si des messages d'erreurs sont apparus dans l'intervalle, tels que « *Erreur d'entrée/sortie* » ou « *Input/output error* », cela indique que la sauvegarde est corrompue. En règle générale, il faut alors se débarrasser du support (CD ou DVD, clé USB ou disque dur), en prendre un autre et refaire une nouvelle sauvegarde.

Note : ces deux méthodes partagent le défaut de ne pas vérifier l'intégrité des données. Mettre en place un mécanisme pour le faire est difficile sans recourir à des logiciels de sauvegarde plus complexes.

page 41

19.2 En utilisant Déjà Dup

🕒 *Durée* : 5 minutes pour installer le logiciel.

On peut également préférer utiliser un logiciel spécialisé dans la réalisation des sauvegardes. L'un d'entre eux, baptisé « Déjà Dup », a comme avantages d'être facile à utiliser, et de réaliser des sauvegardes chiffrées. Ces sauvegardes sont également « incrémentales », c'est-à-dire que les fichiers inchangés depuis la sauvegarde précédente ne sont pas copiés une nouvelle fois, et qu'il est possible d'accéder aux fichiers tels qu'ils étaient à chacune des sauvegardes.

Ce qui le rend aussi simple peut être aussi une limite : il ne sait gérer qu'une seule configuration à la fois. On ne peut donc pas sauvegarder des dossiers différents sur des supports différents à des fréquences différentes. C'est surtout l'outil idéal pour sauvegarder l'essentiel du contenu de son dossier personnel, mais pas beaucoup plus.

Il n'est pas livré avec l'environnement par défaut, il est donc nécessaire d'installer le paquet `Debian deja-dup` pour pouvoir s'en servir.

page 120

19.2.1 Effectuer une sauvegarde

🔄 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

🕒 *Durée* : 15 minutes environ pour la configuration, de quelques minutes à plusieurs heures pour la sauvegarde, selon la taille de ce qu'on veut copier.

On ouvre Déjà Dup via *Applications* → *Outils systèmes* → *Administration* → *Sauvegarder*.

L'interface est simplissime : deux énormes boutons nous accueillent, l'un pour *restaurer des fichiers d'une sauvegarde précédente*, l'autre pour *Afficher seulement les paramètres de sauvegarde*.

Avant que toute sauvegarde soit possible, il faut donc *Afficher* ces paramètres.

1. Dans le menu de gauche, cliquer sur *Stockage* pour choisir l'emplacement de la sauvegarde, ainsi que le nom du nouveau dossier où elle sera enregistrée.
2. Dans *Dossiers*, on trouve la liste des dossiers à inclure dans la sauvegarde (à gauche), et celle des dossiers à exclure (à droite). Laisser le *Dossier personnel* dans la fenêtre de gauche est suffisant dans la plupart des cas. Dans la liste de droite, on peut rajouter les dossiers contenant des fichiers souvent volumineux, comme *Vidéos* ou *Musique*.
3. Si l'on désire effectuer ces sauvegardes automatiquement, cliquer sur *Planification* pour choisir la fréquence de sauvegarde et la durée de conservation des données.

4. On peut maintenant retourner à la *Vue d'ensemble*. Dans le cas où l'on a choisi une sauvegarde automatique, déplacer le curseur sur la droite pour lancer cette dernière, sinon, cliquer sur *Sauvegarder maintenant*. Une nouvelle fenêtre s'ouvre, nous demandant une phrase de passe pour chiffrer¹ notre nouvelle sauvegarde. une fois la phrase de passe confirmée, cliquer sur *continuer* pour démarrer la sauvegarde.
5. On peut maintenant fermer Déjà Dup. Lors de la prochaine sauvegarde, si les paramètres ne sont pas changés, il suffira de donner la phrase de passe de la sauvegarde pour que cette dernière soit mise à jour.

On peut modifier plus tard tous ces paramètres en redémarrant Déjà Dup.

Lorsque la planification des sauvegardes est activée et que le temps indiqué depuis la précédente sauvegarde est écoulé, Déjà Dup affiche un message de notification pour nous signifier qu'il effectuera la prochaine sauvegarde dès que le support externe sera de nouveau branché sur l'ordinateur. Et dès que ce sera le cas, une fenêtre s'ouvrira automatiquement pour demander de saisir la *phrase de passe* nécessaire pour mettre à jour la sauvegarde.

19.2.2 Restaurer une sauvegarde

- 🔄 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*
- 🕒 *Durée : 5 minutes pour configurer, de quelques minutes à plusieurs heures pour la restauration, selon la taille de nos sauvegardes.*

On ouvre Déjà Dup via *Applications* → *Outils systèmes* → *Administration* → *Sauvegarde*. L'opération de restauration démarre simplement en cliquant sur le bouton *Restaurer*.

Si c'est la première fois qu'on utilise Déjà Dup (par exemple pour restaurer son dossier personnel après la perte d'un disque dur), il nous demande d'indiquer le dossier où ont été effectuées les sauvegardes. Sinon, il utilise le dossier déjà configuré.

Après un court délai, Déjà Dup nous demande de choisir, avec sa date, la sauvegarde à restaurer.

Il faut ensuite indiquer le dossier où seront écrits les fichiers issus de la sauvegarde. On peut soit restaurer vers l'emplacement original (ce qui remplace éventuellement des fichiers par la version qui se trouvait dans la sauvegarde), soit indiquer un autre dossier.

Pour finir, un dernier écran résume les paramètres de cette restauration. Après avoir cliqué sur *Restaurer*, une fenêtre s'ouvre, si nécessaire, pour demander le mot de passe du superutilisateur (par exemple, pour restaurer les permissions de certains fichiers). Si la sauvegarde a été chiffrée, Déjà Dup nous demande ensuite la phrase de passe. Une fois que l'on aura cliqué sur *Continuer*, l'écriture des fichiers en provenance de la sauvegarde commencera pour de bon.

19.2.3 S'assurer que les sauvegardes sont toujours lisibles

- 🔄 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

1. Si le support externe est chiffré, on peut éventuellement décider de ne pas chiffrer les fichiers sauvegardés. Cela fait une phrase de passe de moins à inventer et à retenir. On perd néanmoins la possibilité de compartimenter les accès, au cas où le support externe servirait à d'autres choses que les sauvegardes.

⌚ *Durée : de quelques minutes à plusieurs heures, selon la taille de nos sauvegardes.*

Le fonctionnement incrémental de Déjà Dup assure déjà superficiellement que les sauvegardes précédentes soient lisibles. Néanmoins cela ne constitue pas une garantie...

Malheureusement, la meilleure méthode actuellement disponible avec Déjà Dup pour s'assurer que l'on peut restaurer ses sauvegardes est... de faire une restauration vers un dossier temporaire que l'on effacera après. C'est loin d'être pratique, vu qu'il faut avoir accès à un disque dur chiffré suffisamment grand.

On peut toutefois s'assurer que les fichiers contenant les sauvegardes restent lisibles en utilisant les mêmes méthodes que celles décrites précédemment.

Partager un secret

🔄 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

🕒 *Durée : une heure environ.*

Parfois, on souhaite être plusieurs à partager un secret, sans pour autant que chaque personne ne dispose de la totalité du secret.

Cela tombe bien, plusieurs techniques cryptographiques ont été inventées pour cela. Elles permettent toutes, mais avec des calculs mathématiques un peu différents, de découper un secret en plusieurs morceaux, que l'on pourra reconstituer en réunissant quelques-uns ¹.

20.1 Partager une phrase de passe

L'usage le plus pratique est de partager comme secret la phrase de passe d'un support chiffré. [page 137]

Cette étape doit idéalement être faite à partir d'un système *live* afin de ne pas laisser des traces du secret que l'on va partager. [page 99]

20.1.1 Installer le paquet nécessaire

Pour réaliser le partage du secret, on utilisera le programme `ssss-split`. On trouve ce programme parmi ceux fournis par le système *live Tails*, cependant, pour en disposer sur une Debian chiffrée, il est nécessaire d'installer le paquet Debian `ssss`. [page 120]

Les outils contenus dans le paquet `ssss` sont à utiliser en ligne de commande. Toutes les opérations devront donc être effectuées dans un *Terminal*, sans les pouvoirs d'administration. [page 85]

20.1.2 Générer une phrase de passe aléatoire

Dans notre cas, personne ne doit pouvoir ni se souvenir ni deviner la phrase de passe qui sera utilisée pour le chiffrement. On va donc générer une phrase de passe complètement aléatoire en tapant la commande :



```
head -c 32 /dev/random | base64
```

1. Pour plus de détails, voir l'article de Wikipédia sur les [secrets répartis](https://fr.wikipedia.org/wiki/Secret_réparti) [https://fr.wikipedia.org/wiki/Secret_réparti].

L'ordinateur va répondre quelque chose comme :

```
7rZw00u+8v1stea980uyU1efwNzHaKX9CuZ/TK0bRWY=
```

Si l'on désire une phrase de passe de plus ou moins de 32 caractères, il suffira de remplacer 32 par le nombre de caractères désirés. Sélectionner cette ligne à l'aide de la souris et la copier dans le presse-papiers (via le menu *Édition* → *Copier*).

20.1.3 Découper le secret

Avant de découper le secret, il faut décider en combien de morceaux il sera découpé, et combien de morceaux seront nécessaires pour le reconstituer.

Ensuite, toujours à l'aide de notre terminal, il faut utiliser `ssss-split` de la façon suivante :



```
ssss-split -t NOMBRE_DE_MORCEAUX_NECESSAIRES -n NOMBRE_DE_MORCEAUX_TOTAL
```

Le `NOMBRE_DE_MORCEAUX_NECESSAIRES` est le nombre de morceaux qu'il sera nécessaire de réunir pour retrouver la phrase de passe de départ. Le `NOMBRE_DE_MORCEAUX_TOTAL` correspond au nombre de morceaux en lesquels la phrase de passe sera découpée. Le message `WARNING: couldn't get memory lock` peut être ignoré sans problème si on utilise bien un système *live*.

Lorsqu'il demande le secret, on peut coller le contenu du presse-papier, à l'aide du menu *Édition* → *Coller*. Appuyer ensuite sur la touche *Entrée* pour valider la commande.

Chaque personne partageant le secret devra conserver l'une des lignes affichées ensuite. Cela dans leur **intégralité**, en prenant également bien en note le premier chiffre suivi du tiret.

Voici un exemple avec la clé aléatoire générée précédemment, partagée entre 6 personnes et qui nécessitera que 3 d'entre elles se réunissent pour la retrouver :

```
$ ssss-split -t 3 -n 6
Generating shares using a (3,6) scheme with dynamic security level.
Enter the secret, at most 128 ASCII characters :Using a 352 bit security level.
1-b8d576a1a8091760b18f125e12bb6f2b1f2dd9d93f7072ec69b129b27bb8e97536ea85c7f6dcee7b
↪ 4399ea49
2-af83f0af05fc207e3b466caef30ec4d39c060800371feab93594350b7699a8db9594bfc71ed9cd2b
↪ f314b738
3-4718cb58873dab22d24e526931b061a6ac331613d8fe79b2172213fa767caa57d29a6243ec0e6cf7
↪ 7b6cbb64
4-143a1efcde7f4f5658415a150fcac6da04f697ebfeb9427b59dca57b50ec755510b0e57ccc594e6b
↪ 1a1eeb04
5-fca1250b5cbec40ab14964d2cd7463af34c389f81158d1707b6a838a500977d957be38f83e8eebf7
↪ 9266e74a
6-ebf7a305f14bf3143b801a222cc1c857b7e8582119374925274f9f335d283677f4c002f8d68bcce7
↪ 22ebba1f
```

20.1.4 Créer le support chiffré

On pourra ensuite créer le support chiffré. Au moment d'indiquer la phrase de passe, on pourra copier le contenu du presse-papier, comme précédemment, ou alors la retranscrire en l'ayant sous les yeux.

20.2 Reconstituer la phrase de passe

Afin de reconstituer la phrase de passe, il est nécessaire de disposer d'au moins autant de morceaux que le nombre minimal décidé lors du découpage.

Cette étape doit idéalement être faite à partir d'un système *live* afin de ne pas laisser de traces du secret partagé.

page 99

20.2.1 Installer les paquets nécessaires

Comme précédemment, si le programme n'est pas disponible sur le système on aura besoin d'avoir installé le paquet `ssss` et d'avoir ouvert un terminal.

page 120

20.2.2 Recombiner le secret

Afin de recombinaer le secret, on utilisera le programme `ssss-combine`. Il est nécessaire de lui indiquer le nombre de morceaux qu'on a à notre disposition :



```
ssss-combine -t NOMBRE_DE_MORCEAUX_A_DISPOSITION
```

Le programme demande ensuite de saisir les morceaux à notre disposition. Il faut taper *Entrée* après chacun d'entre eux. Si tout se passe bien, le programme affichera ensuite la phrase de passe complète.

Pour reprendre l'exemple précédent, cela donne :

```
$ ssss-combine -t 3
Enter 3 shares separated by newlines :
Share [1/3] :
↪ 4-143a1efcde7f4f5658415a150fcac6da04f697ebfeb9427b59dca57b50ec755510b0e5
↪ 7ccc594e6b1a1eeb04
Share [2/3] :
↪ 2-af83f0af05fc207e3b466caef30ec4d39c060800371feab93594350b7699a8db9594bf
↪ c71ed9cd2bf314b738
Share [3/3] :
↪ 6-ebf7a305f14bf3143b801a222cc1c857b7e8582119374925274f9f335d283677f4c002
↪ f8d68bcce722ebba1f
Resulting secret :7rZw00u+8v1stea980uyU1efwNzHaKX9CuZ/TK0bRWY=
```



Attention, si un des morceaux a mal été tapé, l'erreur qui s'affiche n'est pas forcément très explicite :

```
$ ssss-combine -t 3
Enter 3 shares separated by newlines :
Share [1/3] :
↪ 4-143a1efcde7f4f5658415a150fcac6da04f697ebfeb9427b59dca57b50ec755510b0e5
↪ 7ccc594e6b1a1eeb04
Share [2/3] :
↪ 2-af83f0af05fc207e3b466caef30ec4d39c060800371feab93594350b7699a8db9594bf
↪ c71ed9cd2bf31ab738
Share [3/3] :
↪ 6-ebf7a305f14bf3143b801a222cc1c857b7e8582119374925274f9f335d283677f4c002
↪ f8d68bcce722ebba1f
Resulting secret :.....L.fm.....6 _...v..w.a....[....zS.....
WARNING :binary data detected, use -x mode instead.
```

20.2.3 Ouvrir le support chiffré

Une fois la phrase de passe obtenue, on peut utiliser un copier/coller afin de déverrouiller le support chiffré, ou alors la retranscrire en l'ayant sous les yeux.

Utiliser les sommes de contrôle

🔄 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

🕒 *Durée : 5 à 10 minutes.*

Dans la première partie, on a évoqué les *sommes de contrôle*, des « nombres » qui permettent de vérifier l'intégrité d'un fichier (ou de toutes autres données). Le principe est qu'il est quasiment impossible d'avoir une somme de contrôle identique pour deux fichiers différents. Si Alice dit à Betty dans une lettre que le programme que cette dernière peut télécharger sur son site a pour somme de contrôle SHA256 171a0233a4112858db23621dd5ffa31d269cbdb4e75bc206ada58ddab444651f et que le fichier qu'elle a reçu a la même somme de contrôle, il est quasiment sûr que personne n'a falsifié le programme en chemin, et elle peut exécuter le programme sans trop de craintes.

page 41

Il existe plusieurs algorithmes pour faire des sommes de contrôles. Parmi eux :

- MD5 n'est plus sûr de nos jours et est à proscrire ;
- SHA1 est très utilisé, mais est en voie d'être cassé. Il faut l'abandonner ;
- SHA224, SHA256, SHA384 et SHA512 sont pour l'instant toujours sûrs. Nous allons utiliser SHA256, mais les mêmes méthodes fonctionnent avec les autres algorithmes.

21.1 Obtenir la somme de contrôle d'un fichier

Que l'on souhaite vérifier l'intégrité d'un fichier, ou permettre à son correspondant de le faire, il faut calculer la somme de contrôle de ce fichier.

page 41

Il est possible d'utiliser un outil graphique tout aussi bien qu'un terminal pour effectuer de tels calculs, nous n'allons cependant pas détailler l'utilisation d'un terminal.

21.1.1 Installer les logiciels nécessaires

Si le paquet `nautilus-gtkhash` n'est pas encore installé, l'installer. Ce paquet est installé par défaut dans *Tails*.

page 120

21.1.2 Utiliser GtkHash

Pour lancer *GtkHash*, aller dans *Applications* → *Accessoires* → *GtkHash*. Une fenêtre s'ouvre proposant de sélectionner un fichier pour lequel des sommes de contrôle seront calculées, avec trois sélections par défaut, MD5, SHA1, SHA256. Si une autre somme de contrôle que celles-ci est nécessaire, aller dans *Édition* → *Préférences* et cocher les

sommes de contrôles désirées pour les voir s'afficher. Une fois cela terminé, cliquer sur le champ contenant (*Aucun*) situé après l'entrée *Fichier* et sélectionner le fichier dont on veut calculer une somme de contrôle. Cliquer enfin sur *Hash*, les sommes de contrôles apparaissent alors.

21.2 Vérifier l'intégrité d'un fichier

Il faut obtenir la somme de contrôle du fichier original par un moyen sûr, autre que celui par lequel on a reçu le fichier. Par exemple, si l'on a téléchargé le fichier, on peut avoir reçu sa somme de contrôle dans une lettre, ou par téléphone — le mieux étant bien sûr de vive voix.

De la même manière, pour permettre à d'autres personnes de vérifier l'intégrité d'un fichier, on leur fera parvenir la somme de contrôle selon les mêmes méthodes.

Grâce à l'une des méthodes ci-dessus, obtenir la somme de contrôle de sa copie du fichier. Prendre garde à utiliser le même algorithme que celui qui a été utilisé par son correspondant. Si l'on utilise SHA1 et qu'il utilise SHA256, on n'aura bien sûr pas la même somme de contrôle. Si notre correspondant nous propose plusieurs sommes de contrôle, préférer l'algorithme le plus dur à casser.

[page préc.]

Vérifier que les deux sommes de contrôle sont les mêmes — c'est un peu long et fastidieux, mais c'est souvent plus simple à deux, ou en les collant l'une en-dessous de l'autre dans un fichier texte.

Installer et utiliser un système virtualisé

Cet ensemble de recettes traite de l'utilisation d'un système d'exploitation virtuel à l'intérieur d'un système GNU/Linux. Elles sont utilisées par le cas d'usage qui parle de travailler sur un document sensible sous Windows.

22.1 Installer VirtualBox

🔄 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

🕒 *Durée : un quart d'heure environ.*

22.1.1 Principe

L'objectif de cette recette est d'installer VirtualBox, un logiciel qui permet de faire tourner un système d'exploitation (appelé invité) à l'intérieur d'un autre (appelé hôte) : on appelle cela de la *virtualisation*. Cette technologie, ainsi qu'une politique de sécurité l'utilisant, est décrite plus avant dans le cas d'usage expliquant comment travailler sur un document sensible sous Windows.

[page 68]

22.1.2 Installer VirtualBox

L'étape suivante est donc d'installer les paquets `virtualbox-qt` et `virtualbox-dkms`.

[page 120]

22.1.3 Vérifier l'installation


Lancer VirtualBox à partir du menu *Applications* → *Accessoires* → *VirtualBox*. Une fenêtre s'ouvre et nous souhaite la bienvenue dans VirtualBox. Refermons-la, car nous avons encore quelques préparatifs à faire avant de nous servir de ce logiciel.


22.1.4 Créer un dossier pour sauvegarder les images propres

Comme expliqué dans le cas d'usage, on aura plus tard envie de sauvegarder des images de systèmes propres. Créons dès maintenant un dossier pour cela, par exemple en ajoutant dans le *Dossier personnel* (accessible depuis le menu *Raccourcis*) un dossier *Disques virtuels propres*.

[page 68]

22.2 Installer un Windows virtualisé

 Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.

 *Durée : 20 minutes environ, plus le temps d'installer Windows (de 30 minutes à plus d'une heure).*

Avant tout chose, se munir d'un CD d'installation de la version de Windows appropriée, et l'insérer dans le lecteur CD/DVD. Si une fenêtre affichant le contenu du CD s'ouvre automatiquement, la refermer ou l'ignorer.

22.2.1 Préparer l'installation sur VirtualBox

Depuis le bureau, aller dans *Applications* → *Accessoires* → *VirtualBox*.

Le programme démarre. Cliquer sur *New* et suivre l'assistant :

- Choisir un *Nom* pour la machine virtuelle.
- Choisir le *Type de l'OS* correspondant parmi les versions de Windows proposées.
- Indiquer la taille de *Mémoire vive* dédiée à la machine virtuelle. Pour Windows, 512 Mio est le minimum recommandé.
- Créer un *Disque dur virtuel* pour accueillir le système d'exploitation virtuel :
 - cocher *Disque d'amorçage* et *Créer un nouveau disque dur* ;
 - une fenêtre s'ouvre, cliquer sur *Suivant* ;
 - choisir *Dynamiquement alloué* (l'image disque s'agrandira au besoin, jusqu'à atteindre au maximum la taille indiquée) ;
 - dans *Emplacement*, donner un nom au fichier image disque (on peut aussi choisir son emplacement en cliquant sur le petit dossier à droite de cette ligne, mais c'est bien de le laisser à l'endroit suggéré) ;
 - choisir la *Taille* de l'image virtuelle : sachant qu'on veut accueillir tout un Windows, elle doit être conséquente ! 20 Go, c'est bien si on a assez de place ; en cas de petit disque dur, essayer moins...
 - cliquer sur *Suivant* puis *Créer* : le logiciel a créé et sélectionné un disque dur virtuel.
- Cliquer sur *Créer*.

Sur la fenêtre principale de VirtualBox, la liste contient maintenant notre nouvelle machine virtuelle. Il reste à y installer le système d'exploitation...



Mais avant tout, on va cliquer sur le bouton *Configuration* : ce menu permettra par la suite de la configurer. Pour l'instant on va juste lui dire deux choses :

1. Il faut couper l'accès au réseau (pour des raisons de sécurité déjà mentionnées) :
 - aller dans la catégorie *Réseau* ;
 - décocher la case *Activer la carte réseau* dans tous les onglets où elle est déjà cochée par défaut (généralement, dans un seul : le premier).
2. Il faut lancer le système sur le CD d'installation de Windows qu'on a mis dans le lecteur CD/DVD :
 - aller dans la catégorie *Stockage* ;
 - dans *Arborescence Stockage*, sélectionner la ligne contenant une icône de CD et intitulée *Vide* ;
 - ensuite, dans *Attributs*, à la ligne *Lecteur CD/DVD*, sélectionner *Lecteur de l'hôte [...]*, ce qui correspond à votre lecteur CD/DVD habituel.

Cliquer ensuite sur *OK* pour enregistrer les paramètres.

22.2.2 Lancer la machine virtuelle

Si ce n'est pas déjà fait, c'est le moment de glisser le CD d'installation de Windows dans le lecteur de l'ordinateur.

En ayant toujours notre nouvelle machine virtuelle sélectionnée, on peut maintenant cliquer sur l'icône *Démarrer*. Le système virtuel démarre... c'est le moment de découvrir l'utilisation de la machine virtuelle.

Lorsqu'elle est lancée, la machine virtuelle fonctionne dans une fenêtre qui permet de gérer son utilisation :

- en haut à gauche : une barre de menus contenant *Machine*, *Écran*, *Périphériques*, *Aide* ;
- en bas à droite : des icônes indiquant comment la machine virtuelle utilise le matériel. On peut par exemple vérifier, en passant la souris dessus, le comportement du curseur de souris entre système hôte et invité.

Au premier clic dans la fenêtre, le logiciel explique qu'il va capturer la souris ; à la première touche tapée, il explique qu'il capture le clavier. Il faut bien prendre en compte ce qu'il indique, c'est ce qui permet de savoir comment par la suite sortir de la machine virtuelle !

Enfin, tout ça est expliqué par le logiciel. Il nous reste donc à installer le Windows virtuel.

22.2.3 Installer Windows

Le système virtuel démarre sur le lecteur CD/DVD qu'on lui a indiqué et commence l'installation.

On ne rentrera pas dans les détails du processus. On peut toutefois préciser :

- Au moment de formater la partition, mieux vaut choisir *Formater avec NTFS (rapide)*.
- Ne pas mettre d'informations personnelles lorsque le *Nom* et l'*Organisation* sont demandés. Mettre par exemple un simple point (« . ») dans les cases permet, la plupart du temps, de continuer l'installation.
- Lors de la configuration du réseau, un message d'erreur peut être affiché. C'est bon signe : nous avons désactivé le réseau de la machine virtuelle.

22.2.4 Démarrer sur le système invité

Une fois l'installation terminée, éteindre la machine virtuelle. Retourner dans la fenêtre principale de VirtualBox. Sélectionner la machine virtuelle qu'on vient d'installer et cliquer sur l'icône *Configuration*. Dans la liste de gauche, choisir *Stockage*. Dans *Arborescence Stockage*, sélectionner la ligne contenant une icône de CD et dans la liste déroulante *Lecteur CD/DVD* choisir *Ejecter le disque du lecteur virtuel*. Fermer alors la fenêtre de configuration.

Démarrer alors la machine virtuelle en cliquant sur *Démarrer*.

22.2.5 Installer les logiciels bonus pour système invité


Dans la fenêtre qui accueille Windows, ouvrir le menu *Périphériques* qui propose d'*Installer les Additions invité...* Si ça n'a pas été fait auparavant, VirtualBox proposera de télécharger l'image ISO qui les contient. Une barre de progression en bas à gauche de la fenêtre indique que le téléchargement est en cours, puis VirtualBox demande *Voulez-vous monter ce CD dans le lecteur virtuel*. Cliquer sur *Insérer*. Un


nouveau CD-ROM est maintenant ajouté à l'environnement de Windows. Si le programme d'installation ne se lance pas automatiquement, il faut lancer *VBoxWindowsAdditions* qui se trouve sur ce nouveau CD-ROM. Reste ensuite à accepter les choix par défaut pour installer les « Additions invité ».

Une nouvelle icône à l'aspect de cube transparent apparaît alors après redémarrage de la machine virtuelle en bas à droite du bureau Windows. Elle signifie que les « Additions » ont été installées.

Éteindre le Windows virtuel. L'installation du Windows virtuel est maintenant terminée.

22.3 Sauvegarder une image de disque virtuel propre

 Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.

 Durée : 10 minutes.

[page 68] Comme indiqué dans la méthode permettant de travailler sur un document sensible sous Windows, on peut avoir besoin de sauvegarder l'image disque d'une machine virtuelle.

22.3.1 Éteindre la machine virtuelle

Si la machine virtuelle propre, qui doit être sauvegardée, est en cours d'utilisation, il faut commencer par l'éteindre (par exemple via le menu *Machine* → *Fermer...* → *Envoyer le signal d'extinction* de VirtualBox, ou, tout bonnement, depuis le menu *Démarrer* de windows).

22.3.2 Ouvrir le dossier des disques virtuels de VirtualBox

Dans le *Dossier personnel*, ouvrir le dossier *VirtualBox VMs*.

22.3.3 Effectuer la sauvegarde

- Sélectionner le disque virtuel dont le nom correspond à celui de la machine virtuelle, par exemple `Windows 2000.vdi`.
- Dans le menu *Édition* choisir *Copier*.
- Aller dans le dossier de sauvegarde des images propres. Si l'on a suivi les conseils donnés précédemment, il s'agit du dossier *Disques virtuels propres* dans *Dossier personnel*.
- Dans le menu *Édition* choisir *Coller* pour obtenir une copie du fichier.
- Sélectionner la copie, et la renommer à partir du menu *Édition* → *Renommer...*. Entrer un nouveau nom, par exemple `Sauvegarde propre de Windows 2000.vdi`.

[page 156]

22.3.4 Effacer la machine virtuelle

On ne va plus se servir de cette machine propre. C'est donc le moment de suivre la recette sur l'effacement d'une machine virtuelle.

[page ci-contre]

22.4 Effacer « pour de vrai » une machine virtuelle

🔄 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

🕒 *Durée : 10 minutes pour supprimer + quelques minutes à quelques heures pour écraser les données.*

Cette recette vise à effacer proprement une machine virtuelle.

22.4.1 Supprimer la machine virtuelle de VirtualBox

Ouvrir la fenêtre principale de VirtualBox, accessible depuis le menu *Applications* → *Accessoires*.

Sélectionner la machine virtuelle à effacer.

Dans le menu *Machine* choisir *Supprimer*, puis choisir *Supprimer de la liste*.

22.4.2 Effacer le disque dur virtuel et son contenu

Ouvrir le dossier des disques virtuels de VirtualBox, *VirtualBox VMs* depuis *Raccourcis* → *Dossier personnel*. Sélectionner le dossier contenant la machine virtuelle à effacer puis utiliser l'outil effacer des fichiers avec leur contenu pour effacer le disque virtuel de la machine virtuelle en question.


page 129


22.4.3 Prévenir VirtualBox que le disque virtuel n'existe plus

Dans le menu *Fichier* de VirtualBox, ouvrir le *Gestionnaire de médias...* puis dans l'onglet *Disques durs*, sélectionner la ligne correspondant au fichier effacé (précédée d'un panneau jaune quelque peu alarmiste), et cliquer sur le bouton *Supprimer*.

Le gestionnaire de médias virtuels, ainsi que la fenêtre de VirtualBox, peuvent maintenant être refermés.

22.5 Créer une nouvelle machine virtuelle à partir d'une image propre

 Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.

 Durée : selon la taille du disque.

page 160

page 68

L'objectif de cette recette est de « décongeler » une image de disque virtuel propre préalablement sauvegardée, afin de l'utiliser pour un nouveau projet, comme le recommande la méthode préconisée pour travailler sur un document sensible sous Windows.

22.5.1 Choix du nom

Il faudra choisir un nom pour cette nouvelle machine virtuelle et les fichiers qui lui correspondent. Ces fichiers étant situés sur le système hôte, ce nom laissera quasi inévitablement des traces dessus, même une fois la machine virtuelle supprimée. Il s'agit donc de choisir ce nom en connaissance de cause.

22.5.2 Copier l'image de disque virtuel

On ne peut pas simplement copier le fichier congelé, car VirtualBox se plaindrait qu'on a deux disques virtuels identiques. Il existe cependant une commande pour recopier un disque virtuel, mais elle n'est accessible que depuis la ligne de commande.

page 85

Commençons donc par ouvrir un terminal (*Applications* → *Accessoires* → *Terminal*).

Ensuite, recopions l'image précédemment décongelée avec la commande :



```
VBoxManage clonehd SAUVEGARDE NOUVEAU_DISQUE
```

Nous allons à présent voir comment construire cette ligne de commande, car il faut remplacer SAUVEGARDE par le chemin d'accès à la sauvegarde du disque virtuel, et NOUVEAU_DISQUE par le chemin du nouveau disque.



Attention ! Si l'on souhaite taper les noms de fichiers à la main, il faut savoir que les chemins sont relatifs au dossier de VirtualBox — si l'on ne change pas les options, il s'agit de `.VirtualBox`. Pour corriger cela, on pourra par exemple mettre des chemins absolus.

La façon la plus simple de faire est de commencer par taper :



```
VBoxManage clonehd
```

Ensuite, il faut ajouter un espace. Puis avec la souris, attraper l'icône du disque virtuel à décongeler (dans le dossier *Disques virtuels propres*) et la lâcher au-dessus du terminal.

Pour ajouter le nouveau disque, on recommence l'opération avec l'icône du dossier *VirtualBox VMs*.

L'affichage devrait à présent ressembler à :



```
VBoxManage clonehd '/home/LOGIN/Disques virtuels propres/Sauvegarde propre de  
↵ Windows XP.vdi' '/home/LOGIN/VirtualBox VMs'
```

Un espace a été ajouté automatiquement avec l'insertion du chemin. On va le supprimer, pour ajouter ensuite le nom du nouveau disque, en écrivant par exemple `/Projet1/Projet1.vdi`.

Au final, cela doit ressembler d'assez près à :



```
VBoxManage clonehd '/home/LOGIN/Disques virtuels propres/Sauvegarde propre de
↳ Windows 2000.vdi' '/home/LOGIN/VirtualBox VMs/Projet1/Projet1.vdi'
```

Après toutes ces étapes, la ligne de commande est complète, et on peut lancer son exécution en tapant sur la touche *Entrée*.

22.5.3 Créer une nouvelle machine virtuelle

Dans le bureau Debian, aller dans *Applications* → *Accessoires* → *VirtualBox*.

Le programme démarre. Cliquer sur *New* et suivre l'assistant :

- choisir un *Nom* pour la machine virtuelle ;
- choisir le *Type de l'OS* correspondant parmi les Windows proposés ;
- choisir la taille de *Mémoire vive* dédiée à la machine virtuelle, en fonction de la quantité dont on a besoin pour le projet prémédité : si on veut utiliser un gros logiciel comme Photoshop, il faut en prévoir le plus possible (au moins 512 Mo), en sachant que VirtualBox râlera si l'on attribue plus de la moitié de la mémoire totale à la machine virtuelle ;
- choisir *Disque d'amorçage* et *Utiliser un disque dur existant*. Cliquer sur l'icône à droite du menu déroulant pour ouvrir une fenêtre qui nous permettra de sélectionner notre image *Projet1.vdi*. Cliquer sur *Ouvrir* ;
- cliquer sur *Suivant* et *Créer*.

Il faut maintenant **avant tout** configurer la machine virtuelle. Cliquer sur le bouton *Configuration* en prenant soin de la sélectionner dans la liste auparavant.

Il faut couper l'accès au réseau (pour des raisons de sécurité déjà mentionnées) :

- Aller dans la section *Réseau* ;
- Décocher la case *Activer la carte réseau* dans tous les onglets où elle est déjà cochée par défaut (généralement, dans un seul : le premier).

Cliquer ensuite sur *OK* pour enregistrer les paramètres.

Créer un compte « utilisateur » pour le nouveau projet

Comme expliqué dans le [cas d'usage](#), on souhaite travailler sur un compte « utilisateur » différent pour chaque projet. Voici comment le faire avec Windows XP — ça ne doit pas être trop différent avec d'autres versions.

page 68

Démarrer la nouvelle machine virtuelle en cliquant sur *Démarrer*.


Une fois dans le Windows virtualisé, ouvrir *Démarrer* → *Panneau de configuration* puis choisir *Comptes d'utilisateurs* et *Créer un nouveau compte*.


Choisir alors un nom pour le nouveau compte, tout en gardant à l'esprit que ce nom sera probablement enregistré dans les documents créés. Choisir ensuite de créer un compte *Administrateur de l'ordinateur*¹ et cliquer sur *Créer un compte*.

Fermer alors la session à partir du menu *Démarrer*. On veillera à ne plus utiliser pour ce projet que le compte nouvellement créé.

1. Étant donné que l'on utilise un disque virtuel propre pour chaque projet et que l'on a pas accès au réseau, cela ne constitue pas un grand risque et nous simplifiera la vie.

22.6 Envoyer des fichiers à un système virtualisé


 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

 *Durée : 10 minutes environ.*

Vu que le Windows *invité* n'a pas le droit de sortir de sa boîte pour aller chercher lui-même des fichiers, il peut être nécessaire de lui en faire parvenir depuis « l'extérieur ». Voyons donc comment procéder.

22.6.1 Depuis un CD ou DVD

C'est nécessaire si on veut installer d'autres logiciels sous Windows virtuel :

- Insérer le CD à lire dans le lecteur, attendre quelques secondes, puis reprendre le contrôle avec le système hôte ( + ou *Home*), et dans la fenêtre accueillant Windows, cliquer sur *Périphérique* puis *Lecteurs CD/DVD* et sélectionner *Lecteur de l'hôte [...]*.
- Windows devrait alors détecter le CD inséré. Si ce n'est pas le cas, on peut aller le chercher dans *Menu Démarrer* → *Poste de travail*. Si ça ne marche pas du premier coup, recommencer l'opération.

On peut ainsi charger les logiciels depuis le lecteur CD de l'ordinateur : il seront installés durablement sur le disque dur virtuel.

22.6.2 Depuis un dossier

Il est possible de rendre un dossier du système hôte lisible par Windows. Mais veillons à ce que ce ne soit pas n'importe quel dossier...

Créer un dossier réservé à cet effet dans le système hôte

Réduire la fenêtre accueillant le système invité. Ensuite, choisir l'emplacement où on veut mettre ce dossier d'échange. Par exemple : dans le *Dossier personnel* faire un clic-droit puis *Créer un dossier* et lui donner un nom évocateur (« *Dossier lisible par Windows* », par exemple).

Indiquer au gestionnaire de la machine virtuelle où se trouve ce dossier

Aller dans la fenêtre de VirtualBox dans laquelle est lancée la machine virtuelle Windows et ouvrir le menu *Périphériques* → *Dossiers partagés...* Ajouter un dossier en cliquant sur l'icône avec un « + » en haut à droite. Une boîte de dialogue s'ouvre :

- dans *Chemin du dossier* cliquer sur *Autre...* et indiquer l'emplacement du dossier à partager ;
- dans *Nom du dossier*, le nom que le dossier aura à l'intérieur du système virtuel s'affiche, par exemple « *partage* ». Il est possible de le modifier, mais ce nom doit être court, et ne doit pas contenir d'espace ;
- cocher la case *Lecture seule*. Ainsi, le système virtuel ne pourra que lire le contenu du dossier, mais rien y écrire ;
- si, et seulement si, le partage de ce dossier doit être permanent, sélectionner *Configuration permanente* ; sinon, le partage ne sera activé que pour cette session.



Attention : avant de valider, il faut être bien sûr que l'on veut laisser le système Windows lire tout le contenu du dossier qu'on a demandé de partager. Si c'est bon, cliquer sur *OK*, et refermer la fenêtre avec *OK*.


Indiquer à Windows XP où se connecter pour trouver ce dossier partagé


- Dans le menu *Démarrer*, ouvrir le *Poste de travail*.
- Dans le menu *Outil*, cliquer sur *Connecter un lecteur réseau*.
- Windows propose un nom de lecteur (par exemple Z:) et demande d'indiquer le dossier : cliquer sur parcourir (à droite) → *VirtualBox Shared Folders* → `\\Vboxsvr` → *Nom_du_repertoire*, puis *OK*. On peut choisir au passage si on veut que ce « lecteur » ne soit accessible que pour la durée de la session en cours, ou à chaque nouvelle session.



Attention : en apprenant à utiliser ce système de partage, on pourrait être tenté de le configurer pour donner accès directement aux périphériques branchés sur le système hôte : c'est bien **la pire idée qu'on puisse avoir**, qui anéantirait à elle seule toute la politique de sécurité.

22.7 Faire sortir des fichiers d'un système virtualisé

 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

 *Durée : 10 minutes environ.*

Le Windows *invité* n'a pas le droit, par défaut, de laisser des traces en dehors de son compartiment étanche. Mais presque inévitablement vient le temps où il est nécessaire d'en faire sortir des fichiers. Voyons donc comment procéder.

22.7.1 En gravant un CD ou DVD

Avant tout, sortir les CD ou les DVD qui pourraient être dans les lecteurs et auxquels on ne veut pas donner accès à la machine virtuelle.

Si la machine virtuelle est en fonction, l'éteindre.

Aller alors dans la fenêtre principale de VirtualBox et sélectionner dans la liste de gauche la machine virtuelle sur laquelle se trouvent les données à graver. Cliquer alors sur l'icône *Configuration*.

Dans la boîte de dialogue *Configuration*, sélectionner *Stockage* dans la liste de gauche, et, dans la section *Arborescence Stockage*, cliquer sur la ligne qui commence par une icône de CD. Dans *Lecteur CD/DVD* choisir *Lecteur de l'hôte* et cocher *Mode direct*. Valider en cliquant sur *Ok*.

Il est alors possible de relancer la machine virtuelle, et de graver les données depuis l'intérieur.

22.7.2 Dans un dossier vide

Il est possible de permettre à Windows d'écrire dans un dossier du système hôte. Mais veillons à ce que ce ne soit pas n'importe quel dossier...



Attention : en apprenant à utiliser ce système de partage, on pourrait être tenté de le configurer pour donner accès directement aux périphériques branchés sur le système hôte : c'est bien **la pire idée qu'on puisse avoir**, qui anéantirait à elle seule toute la politique de sécurité.

Créer un dossier réservé à cet effet dans le système hôte

- Réduire la fenêtre accueillant le système invité.
- Choisir l'emplacement où on veut mettre ce dossier d'échange. Par exemple, dans le *Dossier personnel*, faire un clic-droit puis *Créer un dossier* et lui donner un nom évocateur, comme « *Dossier où Windows peut écrire* ».

Indiquer au gestionnaire de la machine virtuelle où se trouve ce dossier

- Si la machine virtuelle est éteinte, la *démarrer*.
- Aller dans la fenêtre de VirtualBox dans laquelle est lancée la machine virtuelle Windows et ouvrir le menu *Périphériques* → *Dossiers partagés...*
- Ajouter un dossier en cliquant sur l'icône avec un « + » en haut à gauche. Une boîte de dialogue s'ouvre :
 - dans *Chemin du dossier* cliquer sur *Autre...* et indiquer l'emplacement du dossier à partager ;
 - dans *Nom du dossier*, le nom que le dossier aura à l'intérieur du système virtuel s'affiche. Choisir un nom court sans espace, par exemple « *sortie* » ;

- Si on veut exporter un dossier de façon permanente (et non pas pour cette session uniquement) cocher la case *Configuration permanente*;
- ne **pas** cocher la case *Lecture seule*.



Attention : avant de valider, il faut être bien sûr que le dossier en question est vide. Windows pourra en effet non seulement y écrire, mais aussi y lire. Si c'est bon, cliquer sur *OK*, et refermer la fenêtre avec *OK*.

Indiquer à Windows XP où se connecter pour trouver ce dossier partagé

- Dans le menu *Démarrer*, ouvrir le *Poste de travail*.
- Dans le menu *Outils*, cliquer sur *Connecter un lecteur réseau*.
- Windows propose un nom de lecteur (par exemple Z:) et demande d'indiquer le dossier : cliquer sur parcourir (à droite) → *VirtualBox Shared Folders* → `\\Vboxsvr` → *Nom_du_dossier*, puis *OK*. On peut choisir au passage si on veut que ce « lecteur » ne soit accessible que pour la durée de la session en cours, ou à chaque nouvelle session.


Garder un système à jour


Comme expliqué précédemment, les logiciels malveillants se fauillent dans nos ordinateurs, entre autres, par l'intermédiaire de « failles de sécurité ».

page 24

Des corrections pour ces erreurs de programmation (ou de conception) sont régulièrement mises à disposition, au fur et à mesure qu'elles sont identifiées. Une fois que ces corrections sont disponibles, il est particulièrement important de remplacer les anciennes versions des logiciels. En effet, les problèmes corrigés, qui pouvaient n'avoir auparavant été identifiés que par quelques spécialistes, sont ensuite connus et référencés publiquement... donc plus faciles à exploiter.

23.1 Garder Tails à jour

 Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.

 *Durée : 30 minutes à 1 heure, plus environ 30 minutes de téléchargement.*

Un système live étant une collection indivisible de logiciels, exécutés à partir d'un DVD ou d'une clé USB, ou d'une carte SD, la seule solution praticable pour utiliser les dernières versions de ces logiciels est de s'assurer qu'on utilise bien la dernière version du système live.

page 99

Au démarrage du système live Tails, le *Tails upgrader* apparaît pour nous prévenir lorsqu'une nouvelle version qui corrige des failles de sécurité est disponible.

Dans le cas où l'on utilise un DVD, il faut donc détruire celui contenant l'ancienne version et en graver un nouveau. Sauf si celui-ci est réinscriptible, auquel cas il suffira de l'effacer pour y graver la dernière version de Tails.

Pour une clé USB, ou une carte SD, et dans la mesure où l'on dispose d'une connexion Internet, on peut utiliser le *Tails upgrader* directement. Il suffit de cliquer sur *mettre à jour maintenant* et de suivre l'assistant tout au long du processus. Si une erreur se produit, ou s'il est nécessaire d'utiliser une autre méthode de mise à jour, l'assistant nous orientera vers la page de la documentation appropriée.

Celle-ci se trouve facilement à partir de la *Documentation de Tails* se trouvant sur le bureau. Dans le menu à droite, cliquer sur *Documentation*. Dans l'index qui s'ouvre, chercher la section *Premier pas avec Tails* et cliquer sur la page *Mettre à jour une clé USB ou une carte SD Tails*.

23.2 Garder à jour un système chiffré


Une fois installé, un système chiffré doit être gardé à jour pour qu'on puisse continuer


page 105

de lui faire confiance. Les sections qui suivent concernent le système *Debian*, mais les concepts s'appliquent dans les grandes lignes à quasiment tous les autres systèmes.

Le projet *Debian* publie, à peu près tous les deux ans, une version *stable*. Cela représente un énorme effort pour coordonner la compatibilité des différentes versions des logiciels, effectuer de nombreux tests et s'assurer qu'il n'y reste aucun défaut majeur.

23.3 Les mises à jour quotidiennes d'un système chiffré

 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

 *Durée : une minute pour lancer la mise à jour, plus un temps variable pour les téléchargements et l'installation, pendant lequel on peut continuer à utiliser son ordinateur.*

Tout l'intérêt d'une version *stable* de Debian est que par la suite, les logiciels qui la composent ne sont plus modifiés en profondeur : ne seront ajoutées que les améliorations de traduction, les corrections de problèmes liés à la sécurité ou empêchant d'utiliser normalement un programme.


Ces nouvelles versions peuvent donc être en général installées « les yeux fermés », elles ne devraient pas perturber les petites habitudes qu'on a prises.


Lorsqu'on a installé l'*environnement graphique de bureau*, le système vérifiera automatiquement, lorsqu'il sera connecté à Internet¹, la disponibilité de nouvelles versions dans les dépôts configurés.

Lorsque c'est le cas, une fenêtre ainsi qu'une icône apparaîtront dans l'espace de notification afin de proposer de procéder aux mises à jour.

Après avoir cliqué sur l'icône, le système nous demande d'entrer le mot de passe d'administration. Une fois cela fait, une fenêtre s'ouvre avec la liste des paquets qui peuvent être mis à jour. Ils sont normalement tous sélectionnés. Il suffit de cliquer sur le bouton *Installer les mises à jour* (ou en anglais *Install updates*) pour lancer la procédure.

23.4 Passage à une nouvelle version stable

 *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.*

 *Durée : une demie journée à une journée, dont un long temps de téléchargement pendant lequel on peut continuer à utiliser son ordinateur, et un long temps d'installation pendant lequel il vaut mieux ne plus l'utiliser.*

Lorsqu'une nouvelle version *stable* de Debian est sortie, le projet veille à garder à jour la précédente version *stable* pendant une durée d'**un an**.

Il est donc nécessaire de profiter de cette période pour prendre le temps de mettre à jour son système vers cette nouvelle version. C'est un processus plus délicat que les mises à jour quotidiennes – pas nécessairement dans sa réalisation même, mais dans

1. On peut également effectuer ces petites mises à jour (certes un peu moins quotidiennement) sur un ordinateur qui n'aurait pas du tout accès au réseau. Le projet Debian sort régulièrement de nouvelles versions *mineures* (ou *point releases* en anglais) qui sont annoncées sur le site web du projet. Le projet propose alors des DVD contenant tous les paquets mis à jour ; un tel DVD peut par exemple s'appeler `debian-update-7.4.0-amd64-DVD-1.iso`. En ajoutant ce DVD aux *Sources de mise à jour*, il est ensuite possible d'utiliser le *Gestionnaire de mises à jour* sans pour autant que l'ordinateur soit connecté.

le fait qu'il est ensuite nécessaire de s'adapter aux changements qu'auront connus les logiciels que nous utilisons habituellement.

23.4.1 Passage de *Squeeze* à *Wheezy*

La procédure détaillée ici concerne la mise à jour de la version de Debian baptisée *Squeeze* ou 6.0, sortie en février 2011, à la version *Wheezy* ou 7.0, sortie en mai 2013.

Nous documenterons ici une procédure de mise à jour simplifiée qui a été testée sur des installations de Debian *Squeeze* avec un environnement graphique de bureau GNOME et des logiciels provenant uniquement des dépôts officiels de Debian.

Elle nécessite de disposer, pour la durée de la mise à jour, d'une connexion à Internet ou d'un DVD d'installation.

page 106



Attention! Cette procédure simplifiée a moins de chances de fonctionner lorsqu'on a bidouillé son système en ajoutant des sources de mises à jour non officielles.

Si c'est le cas, se référer aux notes de publication officielles du projet Debian², notamment la partie Mises à niveau depuis Debian 6.0 (*Squeeze*)³ et la partie Problèmes à connaître pour *Squeeze*⁴.

Mettre à jour sa Debian *Squeeze*

Avant tout, il est nécessaire de disposer d'une Debian *Squeeze* à jour. Sans cela, la mise à niveau risque fort de ne pas fonctionner. Au cas où ces mises à jour n'auraient pas été faites au quotidien, c'est le moment de rattraper le retard. S'il vous est proposé de redémarrer, suite à de nombreuses mises à jour, le faire avant de procéder à la suite des opérations.

page précédente

S'assurer d'avoir assez d'espace libre sur le disque dur

Avant d'éviter toute mauvaise surprise, il faut avoir au moins 4 Go d'espace libre sur le disque dur qui contient le système.

On peut vérifier cela en ouvrant le *Poste de travail* à partir de menu *Raccourcis*. Ensuite, on effectue un clic-droit sur l'icône du *Système de fichiers* pour atteindre les *Propriétés*. Dans la fenêtre qui s'ouvre, l'information qui nous intéresse se trouve en bas à droite du graphique, avant l'étiquette *libre*.

Libérer de l'espace sur le disque si nécessaire S'il n'y a pas assez d'espace sur le disque dur, une piste est d'effacer d'anciennes mises à jour devenues obsolètes. Pour cela, ouvrir le *Gestionnaire de paquets Synaptic* à partir du menu *Système* → *Administration*. Dans le menu *Configuration* choisir *Préférences*, puis sélectionner l'onglet *Fichiers* et cliquer sur le bouton *Supprimer les paquets en cache*, puis fermer le *Gestionnaire de paquets Synaptic*.

Si cela ne suffit pas, il faudra supprimer certains de nos propres fichiers ou désinstaller des programmes.

Désactiver les autres dépôts Debian

La mise à jour n'est testée qu'avec les paquets officiellement fournis par Debian *Squeeze*. On va donc désactiver tous les autres dépôts Debian, y compris les dépôts *backports* et *volatile*.

page 122

Pour cela, ouvrir les *Sources de mises à jour* à partir du menu *Système* → *Administration*. Vu qu'on va choisir à quels programmes on fait confiance, on doit entrer le

2. <http://www.debian.org/releases/wheezy/i386/release-notes/index.fr.html>

3. <http://www.debian.org/releases/wheezy/i386/release-notes/ch-upgrading.fr.html>

4. <http://www.debian.org/releases/wheezy/i386/release-notes/ch-information.fr.html>

mot de passe d'administration. Dans l'onglet *Third-party software*, décocher tous les dépôts listés, puis cliquer sur *Fermer*.

À ce moment là, si le logiciel demande s'il faut recharger les informations sur les paquets disponibles, lui confirmer en cliquant sur *Actualiser*.

Mettre à jour les dépôts Debian utilisés

Commençons par modifier les dépôts configurés afin d'utiliser ceux dédiés à la nouvelle version. Il n'est pas encore possible de faire cette opération à travers l'interface graphique, il faut donc ouvrir un *Terminal administrateur* et taper la commande suivante :

page 85



```
gedit /etc/apt/sources.list
```

L'éditeur de texte s'ouvre. Dans les menus, on sélectionne ensuite *Rechercher* → *Remplacer*. Dans la fenêtre qui s'ouvre, *Rechercher* « *squeeze* » pour le *Remplacer par* « *wheezy* ». Cliquer ensuite sur le bouton *Tout remplacer*, puis *Fermer* la fenêtre de recherche.

Si une installation ou une mise à jour a été faite auparavant en utilisant un CD ou un DVD, c'est une bonne idée de chercher les lignes qui commencent par « *deb cdrom:* » pour les supprimer.

On peut ensuite quitter l'éditeur en enregistrant les modifications.

Dans une version précédente de ce *guide* on conseillait la création d'un fichier qui n'est plus nécessaire mais pourrait nuire à la mise à jour. Le supprimer grâce à la commande :



```
rm /etc/apt/preferences
```

Si jamais l'ordinateur nous répond *rm: impossible de supprimer « /etc/apt/preferences »: Aucun fichier ou dossier de ce type*, c'est simplement que le fichier est déjà absent.

Nous avons modifié la liste des dépôts ; il faut donc maintenant télécharger la liste des paquets qui y sont disponibles, avant de pouvoir les installer ; pour cela, toujours le *Terminal administrateur* qu'on gardera ouvert, taper la commande :



```
apt-get update
```

Ajouter le DVD d'installation à la liste des dépôts Debian

La méthode la plus simple pour effectuer les mises à jour consiste à laisser Debian les télécharger directement depuis Internet. Au cas où l'ordinateur n'est pas relié à Internet, ou si la connexion est de mauvaise qualité, on peut demander au système d'utiliser un DVD d'installation de Debian comme dépôt de paquets. Si ce n'est pas le cas, passer directement à l'étape suivante.

Pour cela, reprendre le *Terminal administrateur* et taper la commande suivante :



```
apt-cdrom add
```

Il faut ensuite insérer le DVD, et appuyer sur la touche *Entrée*. On peut garder le terminal ouvert, il devrait nous resservir sous peu.

Désactiver l'économiseur d'écran

Lors de la mise à jour, l'économiseur d'écran peut se bloquer, et laisser l'écran verrouillé. Il est donc prudent de le désactiver pour le temps de la mise à jour.

Pour cela, ouvrir *Économiseur d'écran* à partir du menu *Système* → *Préférences*. Dans la fenêtre qui s'ouvre, décocher *Activer l'économiseur d'écran quand l'ordinateur est inactif*. Fermer cette fenêtre.

Lancer la mise à jour proprement dite

La mise à jour se fait en plusieurs étapes que l'on pilotera à l'aide du *Terminal administrateur*.

Notre première commande dit au gestionnaire de paquets, d'une part, que nous préférons qu'il nous pose le moins possible de questions concernant les détails de la mise à jour ; d'autre part, que ces questions doivent être posées dans une interface graphique ; enfin, qu'on ne veut pas voir l'historique des changements :

```
#> export DEBIAN_PRIORITY=critical DEBIAN_FRONTEND=gnome
↵ APT_LISTCHANGES_FRONTEND=none
```

Notre deuxième commande effectue la première partie de la mise à jour du système :

```
#> apt-get upgrade
```

Assez rapidement, le terminal affiche *Souhaitez-vous continuer [0/n] ?* Après avoir confirmé en appuyant sur *Entrée*, on peut voir apparaître une première série de fenêtres nous demandant comment gérer certains changements.

Lorsqu'on ne cherche pas à sortir des choix de Debian, cliquer sur *Suivant* (*Forward* lorsque les choix sont en anglais) à chaque fois est suffisant.

Au bout d'un moment, un certain nombre de paquets ont déjà été mis à jour, et le terminal devrait revenir à l'invite de commande.

La quatrième commande terminera la mise à jour du système :

```
#> apt-get dist-upgrade
```

Encore une confirmation, toujours avec *Entrée*, et c'est parti. On peut voir apparaître une nouvelle série de fenêtres. Sauf à vouloir sortir des propositions de Debian, on cliquera sur *Suivant* (parfois écrit en anglais : *Forward*).

À cette étape de la mise à jour, il peut arriver que le bureau GNOME affiche divers messages d'erreurs. Ce n'est pas particulièrement inquiétant, dans la mesure où l'on est en train de réinstaller de nombreux composants du système. Ces problèmes devraient se résoudre d'eux-mêmes une fois le processus terminé.

Quelques évolutions du système plus tard, le terminal nous invite une nouvelle fois à lui indiquer des commandes.

Quand l'invite réapparaît, on peut alors saisir une dernière commande, pour libérer de l'espace disque :

```
#> apt-get clean
```

Premier redémarrage

Le moment est maintenant venu de redémarrer le système.

Dans notre terminal administrateur, taper la commande `reboot` et appuyer sur la touche *Entrée*.

Réactiver les dépôts Debian supplémentaires

On peut maintenant souffler. Le plus gros est fait. Il reste toutefois encore quelques petits ajustements...

Si l'on a désactivé des dépôts non officiels avant la mise à jour, c'est le moment de vérifier qu'on en a toujours besoin avec la nouvelle version de Debian. Si oui, les réactiver. On peut également réactiver l'économiseur d'écran si on l'a désactivé auparavant.

page 122

Prendre en main le nouveau système.

Après le redémarrage, on se retrouve dans la nouvelle version de Debian. Si l'on a un ordinateur suffisamment puissant, on se retrouve avec un nouvel environnement de bureau appelé *Gnome Shell*, auquel on mettra peut-être un peu de temps à s'habituer. Pour une introduction à cette nouvelle interface, on pourra consulter l'aide en cliquant sur *Activités* en haut à gauche de l'écran puis sur *Applications*, *Accessoires* et enfin *Aide*.

S'assurer que le nouveau système fonctionne correctement


Il peut être utile de s'assurer que les actions et les commandes les plus courantes sont fonctionnelles. Le cas échéant, il pourrait être nécessaire de diagnostiquer et de résoudre les problèmes. Il vaut certainement mieux le faire dès la prise de contact avec le nouveau système, afin de pouvoir repartir pour deux ans avec un système fonctionnel. Les problèmes les plus courants sont souvent décrits, avec les astuces pour les résoudre, dans diverses documentations sur Debian et GNU/Linux.

page 114

Rappelons également qu'il existe des notes de publication officielles du projet Debian⁵.

5. <http://www.debian.org/releases/wheezy/i386/release-notes/index.fr.html>

Nettoyer les métadonnées d'un document


 Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web <https://guide.boum.org/>.

 *Durée : quelques minutes.*

L'objectif de cet outil est d'effacer les métadonnées présentes dans un document avant sa publication. Ces métadonnées ne sont pas les mêmes dans tous les formats de documents : certaines sont plus difficiles (voire impossibles) à nettoyer que d'autres. Cependant, la plupart des formats utilisés pour échanger des documents terminés, que ce soient des textes, des images, du son ou de la vidéo, sont « nettoyables ».

page 21

L'outil qu'on va utiliser ici est le *Metadata Anonymisation Toolkit (MAT)* qui permet de nettoyer aisément de nombreux formats de fichiers.

 **Attention!** Nettoyer les métadonnées n'anonymise pas le contenu des fichiers, et n'enlève pas les éventuels marquages¹ qui seraient inclus dans le contenu lui-même.

24.1 Installer les logiciels nécessaires

Sous Tails, le *Metadata Anonymisation Toolkit* est déjà installé. Sur un système où le paquet `mat` n'est pas encore présent, il faut l'installer.

page 120

24.2 Ouvrir le *Metadata Anonymisation Toolkit*

Aller dans *Applications* → *Outils Système* → *MAT*.

24.3 Ajouter des fichiers à nettoyer

Ajouter le fichier à nettoyer avec *File* → *Ajouter* puis après l'avoir sélectionné cliquer sur *Valider*. Il est également possible de le glisser directement dans *Metadata Anonymisation Toolkit*. On pourra également ajouter plusieurs fichiers et les nettoyer en même temps. Si le logiciel sait nettoyer le fichier sélectionné, il l'ajoute à la liste de fichiers à nettoyer. Passer alors directement à *Scour* (nettoyer les fichiers) ci-dessous.

S'il affiche un message « Fichier(s) non supporté(s) », il faut convertir le document dans un format de fichiers supporté par le *MAT* avec une autre application avant de

1. Voir à ce sujet Wikipédia, 2014, *Tatouage numérique* [https://fr.wikipedia.org/wiki/Tatouage_numérique] et Wikipédia, 2014, *Stéganographie* [<https://fr.wikipedia.org/wiki/Stéganographie>].

pouvoir le nettoyer. La liste des formats supportés est disponible à partir de *Help* → *Supported Formats*.

Souvent, il suffit de l'exporter dans un format d'échange de fichiers commun. Ainsi, le *MAT* ne peut pas nettoyer le fichier *XCF* du programme de manipulation d'images GIMP, mais il sait nettoyer les images exportées en *JPEG* ou *PNG*.

24.4 Nettoyer les fichiers

Une fois le fichier ajouté, le nettoyer avec *Process* → *Scour*. On peut alors fermer *Metadata Anonymisation Toolkit*.

Pour supprimer les fichiers contenant les métadonnées, voir l'outil expliquant comment effacer des fichiers et leur contenu.

Qui parle ?

D'où vient cet ouvrage ? Qui parle, en ses lignes ?

Nous pourrions nous contenter de dire qu'il nous semble parfaitement inintéressant de chercher des réponses à de telles interrogations ; que nous laissons aux flics, spécialistes de la question, le privilège de s'y consacrer ; que nous avons mieux à faire.

Le fait que telle ou telle personne couche des mots sur le papier n'est pas, croyons-nous, particulièrement déterminant dans le contenu d'un texte, dans son existence même.

Nous croyons plutôt qu'il s'écrit lorsque des désirs s'entremêlent, lorsque des nécessités se confrontent, lorsque des questions appellent des réponses. Des façons de se rapporter à ce qui nous entoure se rencontrent, se partagent, se transforment alors. Elles se lient, et des manières *communes* de s'y rapporter se construisent, qui interagissent avec d'autres : cela va des conflits aux complicités, en passant par l'alliance et le clin d'œil entendu ; sont alors en jeu sensibilités, critères éthiques, calculs stratégiques...

Bien plus que la « pensée » de X ou Y, un livre exprime l'état de ces interactions, à un certain moment.

*
* *

Deux caractéristiques de cet ouvrage nous obligent néanmoins à faire face, sous certains angles, aux interrogations relatives à sa provenance. Cet ouvrage prétend d'une part transmettre des savoirs et savoirs-faire techniques, réservés d'ordinaire à de rares spécialistes. D'autre part, la justesse des indications fournies peut avoir de larges implications sur la sérénité des personnes qui les mettraient en œuvre. Les petites erreurs qui nous auront échappé peuvent donc avoir de graves conséquences.

Il importe donc de dire quelques mots sur les bouches qui ont prêté leurs voix à ce guide. Mettre au clair l'étendue de nos savoirs(-faire) — et leurs limites — permet de trouver un rapport d'apprentissage plus adéquat à cet écrit, mais aussi de décider du niveau de confiance *technique* qu'il mérite. Disons donc que, collectivement :

- les questions brassées par ce guide nous traversent, techniquement et politiquement, depuis une dizaine d'années ;
- nous connaissons très bien le fonctionnement des systèmes d'exploitation, et particulièrement celui de Debian GNU/Linux ;
- nous avons des bases solides en cryptographie, mais sommes très loin de pouvoir prétendre à une quelconque expertise en la matière.

Et pour finir, affirmons une dernière fois que la parole portée par cet ouvrage, comme toute parole de *guide*, se doit d'être prise avec des pincettes d'autant plus longues que ses implications sont importantes.

Index

A

algorithme, 38
application, 15
architecture, 11
archivage, 77
argument, 86
authenticité, 41

B

backdoor, voir porte dérobée
backports, 123
bibliothèque, 15
binaire, 11
BIOS, 13, 61
boot, voir démarrage
bug, 20

C

cache, 33
carte-mère, 10
chemin d'un fichier, 86
cheval de Troie, 24
chiffrement, 37
 chiffrer un système, 105
 chiffrer une clé, 137
clé de chiffrement, 38, 40
code source, 29
cold boot attack, 19, 40, 61
collision, 42
confidentialité, 37
CPU, voir processeur
cryptanalyse, 37
cryptographie, 37
 cryptographie asymétrique, 43
 cryptographie symétrique, 43
cryptologie, 40

D

Debian, 15, 105
Déjà Dup, 145
démarrage, 93
disque dur, 12, 32
distribution, 30

dépôt de paquets, 122

E

écrasement des données, 32
effacement, 32
électricité, 14
empreinte, voir somme de contrôle
en-tête LUKS, 40
enregistreur de frappe, 26
espace d'échange, voir mémoire virtuelle
ext2, *ext3*, 16

F

FAT32, 16
fonction de hachage, 42
force brute, 63
format de fichiers, 17
formatage, 16, 34

G

GNU/Linux, 15, 30
GnuPG, 39

H

hachage, 42
HADOPI, 25
hibernation, 20
historique, 20

I

imprimante, 27
installation d'un logiciel, 115
installation d'un système, 105
installeur, 105
intégrité, 41

J

journal, 20
journalisation, 33

K

keylogger, voir enregistreur de frappe

L

library, voir bibliothèque
 licence libre, 30
 licence propriétaire, 29
 ligne de commande, 85
 liste blanche, 53
 liste noire, 53
log, voir journaux
 logiciel, 14

- logiciel espion, 24
- logiciel libre, 29, 30
- logiciel malveillant, 24, 62
- logiciel open source, 30
- logiciel portable, 34
- logiciel propriétaire, 29

 logiciel malveillant, 23
 LOPPSI 2, 23
 LUKS, 40, 137

M

malware, voir logiciel malveillant
 mémoire *flash*, 13, 32, 128
 mémoire morte, voir mémoire persis-
 tante
 mémoire persistante, 12
 mémoire virtuelle, 17, 19
 mémoire vive, 11, 19
 micrologiciel, 13, 61
 mise à jour, 169
 mot de passe, 31
 méta-données, 21

N

noyau, 15
 NTFS, 16
 numérisation, 10

O

ondes, 14
open source, 30
 option, 86
 OS, voir système d'exploitation

P

paquet Debian, 115
 partition, 16
 phrase de passe, 37, 91
 pilote, 15
 politique de sécurité, 51
 porte dérobée, 29
 pourriel, 23, 24
 processeur, 10
 programme, 14
 périphérique, 13

R

RAM, voir mémoire vive
rootkit, 24

S

sauvegarde, 143
 sauvegardes automatiques, 21
secure-delete, 127
sfill, 135
shred, 131, 134
 signature numérique, 44
 signature stéganographique, 27
 somme de contrôle, 41, 153
spam, voir pourriel
spyware, voir logiciel espion
 SSD, voir mémoire *flash*
 stéganographie, 27
swap, 17, 19
 Synaptic, 116, 120
 syntaxe, 86
 système de fichiers, 16, 33
 système d'exploitation, 15

- système hôte, 70
- système invité, 70
- système *live*, 34, 68, 99

T

terminal, 85
 traces, 19
 transistor, 10
 Transmission, 100
 TrueCrypt, 30

U

UEFI, 13, 61
upgrade, voir mise à jour
 USB, 13

V

veille, 20
 VirtualBox, 70, 156
 virtualisation, 69
 virus, 24

W

watermarking, voir signature stégano-
 graphique
 Windows, 68, 157
wipe, voir écrasement des données

Photo page 10 de Darkone, licence CC BY-SA 2.5, trouvée sur :
[https://secure.wikimedia.org/wikipedia/fr/wiki/Fichier:
ASRock_K7VT4A_Pro_Mainboard.jpg](https://secure.wikimedia.org/wikipedia/fr/wiki/Fichier:ASRock_K7VT4A_Pro_Mainboard.jpg).

Photo page 10, domaine public, trouvée sur :
<https://secure.wikimedia.org/wikipedia/fr/wiki/Fichier:Pentium-60-back.jpg>

Photo page 12, domaine public, trouvée sur :
https://secure.wikimedia.org/wikipedia/fr/wiki/Fichier:DDR_RAM-3.jpg

Photo page 12, domaine public, trouvée sur :
<https://secure.wikimedia.org/wikipedia/fr/wiki/Fichier:Hdd-wcsi.jpg>

Photo page 13 de Zac Luzader Codeczero, licence CC BY 3.0, trouvée sur :
[https://secure.wikimedia.org/wikipedia/fr/wiki/Fichier:
AT_Motherboard_RTC_and_BIOS.jpg](https://secure.wikimedia.org/wikipedia/fr/wiki/Fichier:AT_Motherboard_RTC_and_BIOS.jpg).

guide d'autodéfense numérique

tome 1

hors connexions

« [...] nous n'avons pas envie d'être contrôlables par quelque « Big Brother » que ce soit. Qu'il existe déjà ou que l'on anticipe son émergence, le mieux est sans doute de faire en sorte qu'il ne puisse pas utiliser, contre nous, tous ces merveilleux outils que nous offrent — ou que lui offrent — les technologies numériques. [...] »

Même si l'on choisit de ne pas les utiliser directement, d'autres le font pour nous. Alors, autant essayer de comprendre ce que ça implique.

Face à ces constats, la seule voie praticable semble être de devenir capables d'imaginer et de mettre en place des politiques de sécurité adéquates.

Tout l'enjeu de ce guide est de fournir cartes, sextant et boussole à quiconque veut cheminer sur cette route.

Ce premier tome se concentre sur l'utilisation d'un ordinateur « hors connexion » — on pourrait aussi bien dire préalablement à toute connexion : les connaissances générales qu'il apporte valent que l'ordinateur soit connecté ou non à un réseau.

Un livre à lire, relire, pratiquer, en solitaire ou à plusieurs, à faire découvrir et à partager... ou comment affiner l'art de la navigation dans les eaux troubles du monde numérique.