Charte de bon usage des moyens informatiques
Annexes

$Id: exegese-all.tex,v 1.4 2001/10/09 12:24:57 pc Exp $

Table des matières

Service Informatique, 23-24 pièce 411, 2 place Jussieu, 75005 Paris,
tél. & fax : 01.44.27.81.57, mailto:admin@eila.jussieu.fr,
http://admin.eila.jussieu.fr

1 Charte de bon usage de l'UFR EILA – Compléments

1.1 Domaine d'application

La charte est en vigueur au sein de l'UFR EILA de l'Université Paris 7 Denis DIDEROT. Elle s'applique à tout matériel informatique de l'UFR, que ce soit pour une utilisation locale ou *via* le réseau, depuis l'intérieur ou l'extérieur des locaux.

1.2 Accès

Chaque utilisateur reçoit en contrepartie de la signature de la charte le droit d'accéder aux matériels que l'UFR met à sa disposition. Il obtient donc un nom d'utilisateur, le mot de passe associé et, éventuellement, un code pour accéder aux locaux. Ce droit d'accès est uniquement accordé pour permettre à l'utilisateur de participer aux activités d'enseignement, de recherche et d'administration et ce, à l'exclusion de toute autre, notamment ludique ou commerciale.

Le mot de passe étant personnel et incessible, l'utilisateur ne doit pas le communiquer à une tierce personne. De plus, l'utilisateur préviendra le responsable informatique si un code d'accès ne lui permet plus de se connecter ou s'il soupçonne que son compte a été usurpé. D'une façon plus générale, il informera le responsable informatique de toute anomalie qu'il pourrait constater.

L'accès aux ressources informatiques est strictement personnel. Il a cours tant que l'utilisateur est inscrit à l'UFR. Il cesse lorsqu'il quitte l'UFR ou s'il est avéré que de dernier a enfreint la présente charte. Il peut être modifié lorsqu'il change de statut au sein de l'UFR.

1.3 Logiciels

L'utilisateur ne doit en aucun cas installer de logiciels sur les plateformes qui lui sont confiées —qu'ils proviennent d'Internet, d'une disquette, d'un CD-ROM ou d'ailleurs—, sans en avoir référé au préalable au responsable du service informatique. De plus, il s'engage à vérifier systématiquement toute donnée entrant sur le réseau de l'UFR par quelque *medium* que ce soit, à l'aide des anti-*virus* mis à sa disposition.

De plus l'utilisateur est tenu de se plier à la législation en vigueur concernant la propriété intellectuelle et commerciale.

1.4 Courrier

L'utilisateur dispose d'une boîte aux lettres électronique. La taille de celle-ci est limitée. Pour éviter des dysfonctionnements du service de messagerie, le service informatique pourra être amené à supprimer les messages les plus anciens dans le cas où les boîtes aux lettres ont atteint une taille maximale. D'une façon plus générale, des modifications des paramètres de messagerie pourront être faites pour assurer le bon fonctionnement. L'utilisateur est expressement prévenu que tout courrier entrant ou sortant est ouvert, que tout courrier contenant un *virus* sera bloqué et signalé à l'auteur et au(x) destinataire(s).

Malheureusement la législation française est très vague au sujet des anti-*virus* mis en place sur les serveurs de courrier. En effet, elle ne différencie pas l'ouverture automatique (par des moyens logiciels) de l'ouverture manuelle (par un tiers). Nous avons fait le choix d'en installer un malgré cela, aussi sommes-nous tenus de dire que le courrier est ouvert.

1.5 Publication

L'UFR offre à ses utilisateurs un espace personnel visible depuis tout le *Web*. Il est évident que les données publiées par ce biais, comme par tout autre moyen électronique, respectent la charte de l'UFR, la présente annexe, la charte du réseau RENATER et le droit français. Il est tout aussi évident que cet espace est avant tout destiné à l'enseignement et la recherche, aucunement à des activités mercantiles. La violation de ces règles entrainera la suppression immédiate du compte ainsi que des poursuites éventuelles.

1.6 Responsabilités

Chaque utilisateur accède et utilise les moyens informatiques et le réseau sous sa propre responsabilité. Il reconnaît que toute violation des dispositions de la charte et de la présente annexe, ainsi que, plus généralement, tout dommage de son fait créé à l'UFR, à l'Université ou à des tiers, engagera sa responsabilité, tant sur le plan disciplinaire, que civil ou pénal. De plus, l'utilisateur reconnaît avoir pris connaissance des règles de sécurité liées à l'usage du réseau RENATER, auquel le réseau de l'Université —et par là même, de l'UFR— est connecté et s'engage à en respecter les obligations.

L'UFR déclare mettre en œuvre —par le biais de la charte et des diverses mesures de sécurité physique et logique qui sont les siennes— tous les efforts nécessaires à un bon usage de ses systèmes et du réseau et n'assumer aucune responsabilité au titre des agissements fautifs ou délictueux des utilisateurs auxquels elle fournit un droit d'accès.

L'utilisateur qui contreviendrait aux règles précédemment définies s'expose à la fermeture de son compte informatique, ainsi qu'aux poursuites disciplinaires et pénales, prévues par les textes législatifs et réglementaires en vigueur.

A Références réglementaires

Il faut connaître :

- La loi n°88-19 du 5 janvier 1988 modifiée par la loi n°92-685 du 22 juillet 1992 relative à la fraude informatique a créé des infractions spécifiques en la matière, reprises par les articles 323-1 à 323-7 du code pénal. Ainsi, il est notamment disposé :
  - Art 323-1
    « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 10 000 F d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 200 000 F d'amende ».
  - Art 323-2
    « Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 300 000 F d'amende ».
  - Art 323-3
    « Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement des données qu'il contient est puni de trois ans d'emprisonnement et de 300 000 F d'amende ».
  - Art 323-4
    « La participation à un groupement formé ou à une entente établie en vue de la préparation caractérisée par un ou plusieurs faits matériels, d'une ou plusieurs infractions prévues par les articles 323-1 à 323-3 est punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée ».
  - Art 323-5
    « Les personnes physiques coupables de délits prévus au présent chapitre encourent également les peines complémentaires suivantes :
    1. L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivants les modalités de l'article 131-26 ;
    2. L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle l'infraction a été commise ;
    3. La confiscation de la chose qui a servi ou été destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ;
    4. La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou plusieurs établissements de l'entreprise ayant servi à commettre les faits incriminés ;
    5. L'exclusion pour une durée de cinq ans au plus, des marchés publics ;
    6. L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ;
    7. L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35. »

  - Art 323-7
    « La tentative des délits prévus par les articles 323-1 à 323-3 est punie des mêmes peines ».
- La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (cf. articles 226-16 à 226-24 du code pénal).
- La loi n°85-660 du 3 juillet 1985 relative aux droits d'auteur, a étendu aux logiciels en tant qu'œuvres de l'esprit, la protection prévue par la loi n°57-298 du 11 mars 1957 sur la propriété littéraire et artistique. (cf. notamment article L 335-2 du code de la propriété intellectuelle qui prévoit le délit de contrefaçon des œuvres protégées).

Il faut en outre connaître les articles Art 410-1 et 411-6 (secrets économiques et industriels) et Art 432-9 al et 226-15 al1 (secrets des correspondances écrites, transmises par voie de télécommunications) qui définissent les secrets par nature.

B Chartes

La charte RENATER est disponible ici : `http://www.renater.fr/Services/Procedures/formulaires.htm#Deontologie`

Non, notre charte n'est monstrueuse ! En voici d'autres, en vigueur ailleurs : `http://www.cru.fr/droit-deonto/deontologie/chartes/`. Nous nous sommes plus que largement inspirés de celle de l'Université de Strasbourg.

C La *Netiquette* et les bonnes manières

La *Netiquette* est fixée par la RFC 1855 (*Request For Comments*[1]), classée FYI 28 (*For You Information*) `ftp://ftp.eila.jussieu.fr/rfc/rfc/rfc1855.txt.gz` dont une traduction est lisible là : `http://www.sri.ucl.ac.be/SRI/rfc1855.fr.html` et un autre résumé ici : `http://www-inf.enst.fr/~vercken/netiquette/netiquette.html`. Les règles en vigueur sur *Usenet* (*aka* les *News*) sont un peu plus strictes : `http://usenet-fr.news.eu.org/fr-chartes/netiquette.html`

C.1 Il faut

- respecter la propriété intellectuelle et commerciale : chacun doit s'assurer que son outil de travail ne comporte pas de copies illicites de logiciels, sa responsabilité étant engagée même s'il n'est pas l'auteur de la copie illicite.
- choisir un bon mot de passe et en changer régulièrement,
- utiliser les moyens techniques existants pour protéger ses données (droits d'accès s'ils existent),
- s'identifier clairement sur les serveurs « anonymes » qui le demandent (*FTP* anonyme)

  Les serveurs *FTP* anonymes laissent un accès en lecture seule à leurs archives *via* les comptes `ftp` et `anonymous` dont le mot de passe est une adresse *email* de la forme `annie@nomat.fr`. Par courtoisie, on donne son adresse correcte et non pas `beauf@moyen.com`.

[1] Les RFC forment en quelque sorte les règles en vigueur sur Internet.

– configurer sa messagerie pour que chaque message envoyé comporte une signature très claire

  Une signature peut comporter ce que vous voulez. Souvent on y trouve des coordonnées et/ou une sentence, un proverbe, une citation, *etc*. Le tout ne doit pas dépasser 4 lignes. Il est de bon ton de faire précéder cette signature d'une ligne ne comportant que `"-- "` soit deux tirets et une espace après, sans les guillemets évidemment. Ainsi, les logiciels de messagerie reconnaîtront automatiquement qu'il s'agit d'une signature.

– configurer sa messagerie pour respecter les standards en vigueur

  Le corps des messages que vous envoyez et recevez peut être dans différents formats dont le *Plain Text* ou texte seul, l'HTML et le *Quoted Printable*. Seul le premier est acceptable car lisible par tous et économe. De plus, veillez à ce que vos lignes ne fassent pas plus de 72 caractères.

– se souvenir que l'accès aux serveurs libres (*FTP* anonyme, *Gopher*, *HTTP*, *NNTP*, ...) n'est pas un droit : c'est une courtoisie de l'organisme qui gère chaque serveur. Ne pas en abuser et rester courtois en cas d'échec.
– essayer de trouver l'information localement (ou à proximité) avant de la rechercher de l'autre côté de la planète : les serveurs importants sont souvent dupliqués (sites miroirs), et plusieurs sites en France sont miroirs de grandes archives (LIP6, INRIA, Rennes, Lyon, *etc.*). Cela permet de désengorger d'autant le réseau.

C.2 Il vaut mieux ne pas

– s'emporter ou mettre en cause injustement une personne ou un groupe dans un message électronique : nul ne sait jusqu'où peut aller un message, surtout s'il est envoyé à une conférence électronique...
– envoyer à une conférence électronique ou un groupe de *News* un message sans aucun rapport avec le sujet du groupe en question ; en particulier, ne pas répondre collectivement à un message émanant d'une liste de diffusion lorsque cette réponse ne concerne que l'émetteur du message,
– poser sur une conférence électronique ou un groupe de *News* une question récurrente et/ou évidente

  Pour éviter cela on se contente de lire les messages pendant quelques jours et on cherche une éventuelle FAQ (*Foire Aux Questions*). Évidemment, ne demandez pas aux autres de faire le boulot à votre place.

– répondre durement à une question « évidente » d'un débutant : on a toujours quelque chose à apprendre, ne serait-ce que la modestie,
– répondre à un message en tapant votre réponse avant la citation

  Les logiciels de messagerie ont une fonction permettant d'inclure automatiquement le texte du message auquel on répond (en le mettant éventuellement en valeur). Étant donné qu'on ne répond pas avant qu'une question soit posée, on ne place pas le texte de sa réponse avant la citation. Le mieux est d'insérer sa réponse au milieu du texte initial, en le mettant en valeur (par des lignes vides par exemple).

– répondre par trois mots à un message en incluant cent lignes de citation inutile

> Vous avez un accès illimité et gratuit *via* un réseau universitaire (très rapide) mais il y a des gens n'ont qu'un accès téléphonique —jusqu'à 1000 fois plus lent— à Internet aussi le chargement de ces lignes inutiles leur coûtera quelques secondes de téléchargement. Si tous les messages qu'ils reçoivent sont de cet acabit, leur facture sera lourde...

– envoyer d'énormes pièces jointes (surtout si elles ne sont pas compressées) ou des fichiers que le destinataire ne pourra lire qu'avec un logiciel non standard et coûteux,
– écrire EN CAPITALES, cela équivaut à CRIER !

C.3 Il ne faut surtout pas

– utiliser un mot de passe simpliste, l'écrire sous le clavier ou le communiquer à un tiers « pour rendre service »,

> *Cf.* plus loin.

– quitter son poste de travail sans terminer sa session,

> L'utilisateur suivant aura alors accès à vos fichiers, votre courrier...

– communiquer le contenu du fichier des mots de passe à un tiers,

> Croyez-vous vraiment que ce soit par curiosité qu'il vous l'a demandé ?

– envoyer un courrier électronique en usurpant la signature d'un tiers

> C'est un délit très grave : les institutions partenaires n'hésiteront pas à porter l'affaire en justice.

– considérer que ce qui est techniquement possible est *ipso facto* autorisé : par exemple, profiter de l'imprudence ou de l'inexpérience d'un autre utilisateur pour accéder à ses données

> Si votre voisin oublie de fermer sa porte en partant, cela ne vous confère pas le droit de rentrer chez lui.

– permettre à tous l'écriture dans un fichier personnel (surtout exécutable),
– inscrire en clair son mot de passe dans un fichier de configuration (`.netrc`),
– installer sur un système (surtout micro-ordinateurs) des logiciels non autorisés par l'administrateur ou des copies illicites de logiciels commerciaux

> Il est malheureusement courant que les utilisateurs installent sans en référer à quiconque divers logiciels amusants. Dans la majeure partie des cas il s'agit de *virus*. L'administrateur système n'est pas chameau avec vous en vous l'interdisant, il vous protège !

– modifier la configuration d'un système sans l'accord de l'administrateur (déplacer une imprimante, changer un écran, modifier le logiciel système, ...),
– essayer d'acquérir des droits supplémentaires « pour voir si c'est possible »

> Cracker une machine, un mot de passe, capturer l'information sur le réseau, ...sont des délits graves relevant du tribunal pénal.

– utiliser la messagerie dans des actions illicites : harcèlement, publicité ou diffamation, chaînes de messages, ...

> Qui n'a jamais reçu un message d'un inconnu vous demandant de le retransmettre à tous vos amis « pour qu'une petite chilienne puisse recevoir un rein » ou « pour vous prévenir d'un nouveau *virus* très dangereux » (qui n'existe évidemment pas) ? Dans les deux cas, il s'agit juste d'encombrer inutilement le réseau. Le second type de message est plus pernicieux et s'appelle un *hoax*. Ignorez le premier type et demandez conseil à votre administrateur pour le second car il serait étonnant que vous soyez au courant avant lui...

- créer un serveur (`FTP`, `Gopher`, `HTTP`) personnel et le faire passer pour celui d'un institut ou laboratoire : c'est une forme d'usurpation d'identité,
- créer un serveur (`FTP`, `Gopher`, `HTTP`) contenant des informations relatives à des personnes : la loi Informatique et Libertés est très stricte...
- créer un serveur (`FTP`, `Gopher`, `HTTP`) contenant des logiciels protégés, ce qui en facilite la copie illicite par le réseau ; les éditeurs de logiciels n'hésiteront pas à porter l'affaire en justice.

C.4 Il faut absolument

- profiter de ce formidable outil de travail et de ce merveilleux espace de culture, de liberté et de tolérance qu'est le réseau Internet `:-)`

Je ne vais pas m'épancher sur l'histoire d'Internet mais il faut tout de même savoir qu'il est né à la fin des années 70 dans les universités américaines et à l'initiative des armées américaines, de manière complétement anarchique (au sens premier du terme, en témoignent les RFC, les serveurs de *News* ou de `FTP` anonyme, ou encore les logiciels libres) aussi les valeurs de gratuité, d'échange, d'entraide et de liberté y sont elles (encore) prépondérantes. Vous rencontrerez sur Internet —pour combien de temps encore ?— des informaticiens « barbus velus » travaillant bénévolement pour le bien de tous, y compris d'entreprises mercantiles ou d'états policiers.

D Les mots de passe

Votre mot de passe doit rester secret, vous devez être absolument seul à le connaître. Parmi les pratiques courantes qui mettent en péril tout le monde, à commencer par vous mais pas seulement :

- le mot de passe noté sur un *Post-It* sur l'écran,
- le mot de passe noté sur un *Post-It* sous le clavier,
- le mot de passe donné à « un ami »,
- le mot de passe crié d'un bout à l'autre de la pièce,
- *etc*.

Parmi les mots de passe courants qui mettent en péril tout le monde, à commencer par vous mais pas seulement (*bis repetita*) :

- le nom de votre chien,
- le prénom de votre chère moitié,
- votre date de naissance,
- votre lieu de vacances,
- tout mot figurant dans un dictionnaire (quelle que soit la langue),
- *etc*.

D.1 Utilité des mots de passe

On entend souvent dire « mais je n'ai rien à cacher alors pourquoi un mot de passe ? ». Il faut savoir que malgré tous les efforts des informaticiens, un logiciel a toujours des *bugs*. Aussi la connaissance d'un mot de passe, si elle ne confère pas en soi beaucoup de droits, peut permettre illégalement d'en acquérir beaucoup plus, parfois facilement. Ne pas protéger votre mot de passe facilite donc les basses œuvres des pirates et si ces derniers parviennent à leurs fins (prendre le contrôle d'une machine la plupart du temps), rien ne vous garantit qu'ils ne détruiront pas vos fichiers ni ceux de vos collègues (par bêtise, par jeu, par défi, par intérêt ou vengeance, pour signer leur passage, *etc*.) aussi les conséquences peuvent être catastrophiques.

D.2 Ingéniérie sociale

Il est une méthode vieille mais éprouvée pour acquérir un mot de passe : il s'agit de ce que l'on appelle pudiquement l'« ingéniérie sociale ».

Cela consiste par exemple à se faire passer pour l'administrateur (ou un fonctionnaire de police ou ...) et vous demander votre mot de passe sous prétexte de vérifications de données ou que sais-je encore. Ni l'administrateur ni les forces de l'ordre (qui s'adresseront à votre administrateur) n'en ont besoin, même pour lire ou modifier vos fichiers. Aussi, ne donnez jamais votre mot de passe à quiconque, quel que soit le prétexte (toujours mauvais).

Cela consiste aussi à utiliser divers renseignements sur vous (nom de votre chien, prénom de votre chère moitié, date de naissance, lieu de vacances) pour deviner votre mot de passe.

D.3 Choisir un mot de passe

Choisir un bon mot de passe demande de l'imagination. Parmi les méthodes probablement les plus sûres, je vous propose celle-ci : apprenez par cœur (si ce n'est pas déjà fait) quelques vers (pas trop connus non plus). Choisissez les initiales de chaque mot de l'un d'eux pour chaque nouveau mot de passe. Une variante consiste à utiliser le nombre de lettres de chaque mot du ver ; mis bout à bout cela forme un nombre complexe. Une autre méthode consiste à utiliser des noms de lieux dits ou des mots de patois mais c'est évidemment moins sûr.

Exemple `Mais qu'allait-il donc faire dans cette galère?` donne `mqaidfcg` ou `mQaiDfcG` avec la première méthode et `426245456` avec sa variante. Évidemment vous ne recopierez pas cet exemple !

Un bon mot de passe fait au strict minimum 6 ou 7 caractères. S'il est trop court, le nombre de combinaisons possibles rend envisageable une attaque exhaustive (le temps de calcul est de l'ordre de la minute pour 3 caractères sur une machine relativement moderne).

Deplus, il faut mélanger minuscules, majuscules, chiffres et signes de ponctuations courants `@#&"'(!)-_^\$*%+=/:;.?,<>|` mais évitez comme la peste les carac-

tères accentués[2] et d'espacement[3].

Un mot de passe se change au moins une fois l'an.

D.4 Validité

Parmi les méthodes d'attaques des accès, la plus répandue est l'« attaque par dictionnaire ». Cela consiste à tenter tout mot de passe potentiel en utilisant une liste de mots courants. Avec la puissance accrue des ordinateurs, il devient de plus en plus facile et rapide de casser un mot de passe d'où ces précautions.

Il est courant que l'administrateur système tente de cracker votre mot de passe par attaque exhaustive ou par dictionnaire pour s'assurer qu'il résistera suffisament longtemps. Si ce n'est pas le cas, attendez vous à ce qu'il vous demande d'en changer.

E Confidentialité

E.1 Cryptographie

Différents moyens cryptographiques sont mis à la disposition des utilisateurs. Pendant longtemps ils ont été considérés comme des armes de guerre dans différents pays dont les États-Unis, la Russie et la France. Désormais l'usage de la cryptographie en France est limitée à des clefs de 128 bits (depuis le 17 mars 1999, décret 99-199 corrigeant la loi 90-1170 du 29 décembre 1990 modifiée sur la réglementation des télécommunications, notamment son article 28). Son usage est recommandé par le Parlement Européen depuis les révélations sur le réseau « Echelon ». Cette limite de 128 bits n'est valable dans la loi française que pour des données intelligibles aussi des logiciels tels que PGP, GnuPG ou OpenSSH sont-ils légaux quand bien même ils utilisent des clefs de 4096 bits, car ce qu'ils chiffrent aussi fortement n'est que la clef de session (de 128 bits) et non pas les données chiffrées à 128 bits à l'aide de cette clef de session.

Si vous n'avez rien compris à cette prose, je vous recommande la lecture de `http://www.scssi.gouv.fr/fr/sciences/crypto/index.html`, du mémoire de terminologie de Johan FESTY (DESS ILTS, promotion 2000-2001) ou encore de la bibliographie commentée de Yamina ABDALLAHI `http://admin.-eila.jussieu.fr/~pc/files/crypto.pdf`. La réglementation en vigueur est décrite ici : `http://www.scssi.gouv.fr/fr/reglementation/legal-.html` et une synthèse est disponible là : `http://www.scssi.gouv.fr/fr/-reglementation/tab_synth.html`.

Vous êtes vivement invités à utiliser des outils cryptographiques plutôt que leurs équivalents classiques chaque fois que cela est possible.

[2] Car ils sont gérés différemment suivant les environnements et les logiciels systèmes.

[3] Souvent considérés comme des séparateurs ; donc si vous en mettez un, certains logiciels considéreront que l'espace marque la fin.

E.2 Traces

L'ensemble des services utilisés génèrent, à l'occasion de leur emploi, des traces qui vont s'enregistrer dans des fichiers. Ces derniers sont essentiels à l'administration des systèmes. Ils servent en effet à diagnostiquer les dysfonctionnements éventuels. Ces fichiers conservent des informations concernant par exemple la messagerie (expéditeur, destinataire(s), date), mais aussi les heures de connexion aux applications de gestion, au service de connexion à distance, le numéro de la machine depuis laquelle les services sont utilisés, *etc*. Ce type de traces existe pour l'ensemble des services Internet. Ces fichiers ne sont utilisés que pour un usage technique. Toutefois, dans le cadre d'une procédure judiciaire et, après accord du Directeur de l'UFR, ces fichiers peuvent être mis à la disposition ou transmis à la Justice.

F Références

La charte est basée sur celle de l'Université Louis PASTEUR de Strasbourg, une partie de l'annexe sur celle de l'Université Paris V René DESCARTES. Nous nous sommes en outre appuyés sur diverses autres chartes en vigueur dans les Universités françaises, à commencer par celle de Nancy 2 Henri POINCARÉ. La partie sur la *Netiquette* est issue d'un document dont nous ne retrouvons plus l'origine ni l'auteur, et que nous avons remanié, complété et commenté.

Pour ceux qui voudraient voir ce que l'indifférence à propos des mesures de sécurité peut entrainer, qu'ils lisent le roman *Hell's r00ts* ; il est téléchargeable : `http://www.kitetoa.com/Les_Livres/Roman/sommaire_roman.shtml` et lisible en ligne là `http://www.kitetoa.com/Les_Livres/Roman/HElls_HTML/sommaire.htm`. Si ce roman se veut être un *scenario* catastrophe de science-fiction, il n'en demeure pas moins que 90 % des procédés techniques relatés existent réellement. Ce n'est pas de la grande littérature mais ça mérite d'être lu et c'est plein de suspens.

Pour ceux que l'histoire de l'informatique, du réseau et des logiciels libres intéresse, ils trouveront des éléments là : `http://www.oreilly.fr/divers/tribune-libre/index.html`.