Sécurité des messages

Bon, nous allons parler de la sécurité des messages. Ce sujet est un peu plus complexe, ce n'est pas grave si tu ne comprends pas tout. Je vais essayer de faire le plus simple possible. Nous approfondirons probablement certaines de ces notions plus tard.

Fais de ton mieux.

De toutes façons j'ai confiance en toi et si je ne comprends pas, on pourra effectivement reprendre plus tard.

Bon, voilà déjà quelques éléments à comprendre.

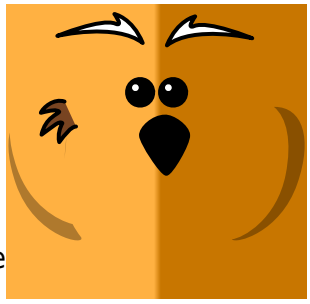
Comme je te l'ai dit, la transmission du message se fait en texte brut. Ce message n'est donc pas qu'un texte intelligible en soi. On dira, pour être plus précis, qu'il s'agit d'une “information”. On transmet une information d'un ordinateur à un autre. Si tu t'intéresses aux théories mathématiques et scientifiques, tu peux aller voir la théorie de l'information de Shannon.

L'information n'est pas simplement transmise comme ça, par magie. Elle est contenue dans un fichier texte, comme, par exemple, avec l'extension `.txt`. Ce qui est très important de retenir c'est que ce type de fichier n'est pas “exécutable”. Par conséquent, si un code malveillant (un virus par exemple) y est contenu, celui-ci ne présentera pas de danger particulier, car il se présentera que comme un code source inerte pour la machine. Il serait nécessaire d'exécuter ce code pour qu'il infecte la machine.

Ok, alors 2 choses :

1. ce qui est transmis est une information qui peut être un message intelligible par les humains, mais cela peut aussi être autre chose si je comprends tout bien ;
2. cette information est contenue dans un *fichier texte* de type `.txt` qui n'est pas exécutable.

Ok, tu peux poursuivre...



Pour qu'un courriel puisse contenir une mise en forme, il faut lui ajouter un code qui sera interprétable. C'est le Web qui lui offrira ce code. C'est ce que l'on a vu à la page précédente. Ainsi, les courriels transmis avec une mise en forme sont en réalité des fichiers `.txt` avec un langage de balisage. C'est le langage HTML qui est utilisé. Ce courriel est donc une pseudo-page Web, un pseudo-fichier `.html`. Le logiciel Client de messagerie se transforme, dans ce cas, en un pseudo navigateur web qui lit et interprète ce code pour rendre une mise en page plus ou moins conforme à la volonté de l'expéditeur.

Cela n'a rien d'anodin et peut avoir de lourdes conséquences, surtout en matière de sécurité. En effet, si le *client de messagerie* est de plus en plus similaire à un *navigateur Web*, c'est qu'il est aussi en mesure de rendre exécutable certains codes, à ton insu, comme le code JavaScript par exemple.

Il faut encore prendre en compte les pièces jointes aux courriels. En fait, il faut aujourd'hui considérer deux types de pièces jointes, même si techniquement c'est la même chose. Il y a d'une part les pièces jointes “classiques” comme les documents `.pdf` par exemple, mais il y a aussi tous les éléments contenus dans le message qui ne sont pas du texte, comme les images affichées, qui sont aussi des pièces jointes. Tous ces éléments sont des pièces jointes qui voyagent en parallèle. C'est comme si le courriel, le *fichier texte*, était une locomotive et que l'on y avait accroché des wagons qui sont ces autres fichiers (`.jpg` et autres `.pdf`). C'est ce petit train qui arrivera dans la boîte de courriel du destinataire.

Outre les pièces jointes, il peut aussi y avoir des éléments externes qui sont liés dans le message. Ces éléments seront récupérés sur un serveur au moment de la lecture du courriel.

Tous ces éléments sont autant de dangers en matière de sécurité informatique pour celui qui reçoit des courriels.

C'est vrai que c'est un peu compliqué là.

Dis-moi si mon résumé est correct :

1. à la page précédente tu disais que les messages sont transmis “en clair”. J'en déduis que le contenu est toujours lisible comme si l'on envoyait une carte postale ;
2. Pour des raisons purement esthétiques qui ne sont par ailleurs pas garanties, des couches de complication sont ajoutées pour permettre des mises en forme et l'intégration d'images directement dans le message, ce qui rend ces courriels dangereux.

C'est très bien résumé.

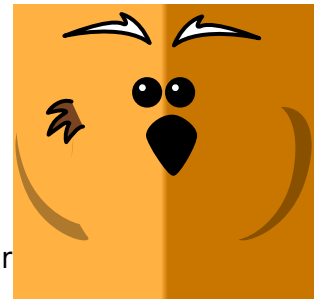
Je finirai par le monopole des grandes entreprises de l'informatique qui ne cessent de tenter de privatiser ces fonctionnalités libres. Par exemple, *Microsoft* à tenter d'imposer, à l'insu de tous, le transfert du contenu des courriels et les pièces jointes dans un fichier `winmail.dat` ou `win.dat`. Ce fichier est alors transmis comme une pièce jointe à un “vrai” courriel, qui lui, ne contient rien. Il s'agit du format TNEF, un format propriétaire, qui n'a aucune utilité et n'apporte aucune protection, ni aucune amélioration d'aucune sorte aux courriels. En fait, ce format ajoute d'autres failles de sécurité. La seule fonction réelle que nous pouvons identifier est d'interdire l'accès aux contenus des courriels et à leurs pièces jointes aux destinataires qui n'adoptent pas ce format !

Si ce format était largement accepté, *Microsoft* aurait pu rendre la fonction de courriel payante. De plus, cela lui offrait des capacités malveillantes envers les utilisateurs. Sans l'intervention des hackers, ce type d'attaques contre les libertés pourraient réussir au même titre que les gens ont adopté volontairement et massivement des ignominies comme *Facebook* ou *gmail* par exemple.

C'est grave ce que tu me dis là...

C'est scandaleux !

Que pouvons-nous faire ?



Pour éviter ce genre de choses, il est nécessaire d'acquérir un minimum de savoir. C'est une lutte contre l'obscurantisme. Le problème est que ce savoir n'est actuellement enseigné dans aucune école. Il faut essayer de suivre les conseils et les mises en garde des hackers et si possible, se former auprès d'eux. Il faut, par ailleurs n'utiliser que des logiciels libres en boycottant tous les logiciels privateurs (propriétaires) de cette industrie malveillante qui est, à ce propos, régulièrement condamné devant les tribunaux du monde entier pour ce type d'agissement !

Je ne vois pas ce que l'on pourrait faire de mieux...