Fiche pratique

La clé de cryptage

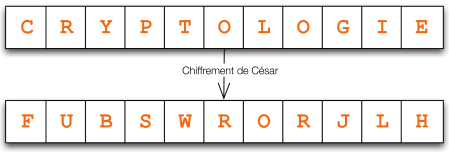
Dans la fiche théorique sur les réseaux WLAN (Wi-Fi) nous avons comparé ces réseaux à un endroit ouvert dans lequel toutes les conversations peuvent être entendues par toutes les personnes se trouvant à proximité. Ceci est une chose contre laquelle il est inutile de lutter puisque c'est la nature même du réseau sans-fil : les ondes voyagent dans les airs et ne peuvent pas être confinées.
Les personnes qui ne veulent pas partager le contenu de leur conversation peuvent faire en sorte de ne pas parler la même langue que les autres personnes présentes, l'Anglais ou l'Allemand par exemple. Cependant rien ne dit qu'une ou plusieurs personnes ne parlent pas cette même langue... Il vous reste à inventer une langue ! C'est l'histoire de l'argot...
En informatique le moyen le plus utilisé pour faire en sorte de protéger ses informations est, quand on ne peut pas les cacher, de les crypter. Ainsi à la lecture ou à « l'écoute », le contenu est parfaitement incompréhensible, même pour celui qui l'a écrit. En revanche, avec la bonne clé il est possible de le décrypter. Voyons de plus près ce qu'est le cryptage.

Mots clés :

- Wi-Fi
- WLAN
- Sans-fil
- Chiffrement
- Cryptage
- WEP
- WPA
- TKIP
- PSK

L'antiquité

On attribue à Jules César (100 av. J-C - 44 av. J-C) le premier « algorithme » de cryptage. Celui-ci faisait parvenir ses ordres à ses troupes situées aux quatre coins du Monde Romain par des messagers. Il était parfaitement conscient du fait que ses messages pouvaient être interceptés par ses ennemis et il était extrêmement important de faire en sorte que ces messages ne puissent être compris. Il inventa un code simple qui rendait incompréhensible son message, mais que le destinataire pouvait interpréter car il en connaissait le code. Le principe était tout simplement de décaler les lettres de l'alphabet de plusieurs lettres. Ainsi le « A » devenait le « C » par exemple, le « B » devenait le « D » et ainsi de suite.



Depuis, les codes sont devenus de plus en plus complexes, de plus en plus mathématiques et aujourd'hui on n'utilise plus ce genre de code rudimentaire mais des codes basés sur des échanges de clés publiques et privées qui ont une longueur non plus de 26 lettres mais de 2048 bits.

DES, RSA, PGP et cie

Ces barbarismes sont des noms d'algorithmes très utilisés pour chiffrer (ou crypter) des séquences binaires ou de texte. Les différences qui les séparent sont de nature algorithmique principalement. Chacun a sa manière d'ordonner, de filtrer et d'appliquer la clé qui fait qu'on ne peut déchiffrer un message avec un algorithme différent de celui utilisé pour le chiffrer, de même qu'on ne peut déchiffrer un message que si on connait la clé utilisée pour le chiffrer. La clé de chiffrement est l'élément variable dans le cryptage. C'est celui qui va vous permettre de différencier votre message d'un autre chiffré avec le même algorithme. Si vous chiffrez un seul poème d'Arthur Rimbaud, deux fois, avec l'algorithme DES et avec deux clés différentes, vous obtiendrez deux résultat différents. Vous ne pourrez ni intervertir les clés, ni utiliser un autre algorithme. En matière de Wi-Fi, les données qui transitent entre deux machines d'un même réseau sont chiffrées à l'aide d'un des protocoles WEP, WPA ou WPA2. Ces protocoles (du plus ancien au plus récent) utilisent des algorithmes de chiffrement différents et en particulier des clés de tailles différentes.

La clé WEP

Le protocole WEP (Wired Equivalent Privacy ou Protection Equivalente au Câble) utilise une clé d'une longueur de 64 à 256 bits dont 24 ne sont pas utilisés pour le chiffrement. Cela fait une clé, si on la compare à un mot, d'une longueur de 5 à 29 caractères. La majorité des clés est composée de 13 caractères. L'algorithme utilisé dans le chiffrement possède une grande faiblesse qui est exploitée aujourd'hui très facilement par les hackers. Il suffit de quelques minutes pour reconstituer tous les morceaux de la clé WEP qui circulent de temps à autres sur votre réseau. La raison pour laquelle ils circulent est intimement liée à l'algorithme utilisé car celui-ci doit être initialisé à chaque échange pour ne pas utiliser deux fois la même clé. De fait une partie de la clé (les 24 bits en question) est utilisée comme élément d'initialisation (vecteur d'initialisation) et celui-ci n'est pas chiffré.

Page suivante >

Au bout d'un moment, si quelqu'un écoute tous les échanges, il aura obtenu suffisamment d'éléments pour reconstruire la clé sans la connaître au préalable. Pour cette raison la clé WEP ne doit absolument plus être utilisée sur les équipements Wi-Fi aujourd'hui.

La clé WPA/WPA2

Le protocole WPA offre une protection d'un niveau bien supérieur à WEP. Il utilise pourtant le même algorithme de chiffrement et est basé sur le même principe de vecteur d'initialisation. En revanche le TKIP (Temporal Key Integrity Protocol ou Protocole d'intégrité par clé temporelle) a été ajouté, permettant ainsi une permutation plus importante des clés sans que le vecteur d'initialisation ne puisse être reconstitué de manière utile.

Dans les configurations les plus courantes, le mode Personnel est utilisé avec la PSK (Pre-Shared Key ou clé pré-partagée). Cela permet d'utiliser une clé alphanumérique normale d'une longueur d'au moins 32 caractères. Ce qui offre un niveau de protection tout à fait acceptable.

Le protocole WPA2 quant à lui utilise un algorithme de chiffrement beaucoup plus puissant, utilisé dans le cryptage des documents sensibles et possédant une clé très forte. Il s'agit de la dernière norme du protocole WPA permettant de protéger votre réseau WLAN.

Malheureusement une faille très importante a été découverte au mois de juillet 2010 dans ce protocole qui reste néanmoins considéré comme le plus sécurisé.

Conclusion

Ne croyez surtout pas qu'une clé WEP, WPA ou même WPA2 vous protège parfaitement, cela n'est pas le cas. Et même si un nouveau protocole WPA3 pouvait offrir une protection acceptable, cela ne durerait qu'un temps. Suivez nos conseils pour paramétrer correctement votre connexion et vos mots de passe, prenez les bonnes habitudes en tant qu'utilisateur de vos logiciels et vous serez protégés durablement !

Repères :

La cryptage est un outil essentiel de la technologie Wi-Fi, puisque c'est lui qui empêchera les personnes indésirables d'espionner les informations que vous communiquez par l'air.

La plupart des box proposent par défaut un cryptage (attention, pas toutes !), mais rien ne vous empêche de l'améliorer si besoin. Certains chiffrements sont en effet obsolètes et facilement crackables, même pour un débutant. C'est le cas par exemple des clés WEP. Préférez donc le cryptage WPA, et a fortiori WPA2, qui résisteront plus longtemps aux éventuelles « attaques ».