LA GESTION DES MOTS DE PASSE

Jacques Supcik

CryptoParty Fribourg - 22 Mars 2014

Puissance actuelle des ordinateurs

- Les ordinateurs sont de plus en plus rapides
- Il y en a toujours plus (certaines organisations possèdent plus de 1'000'000 d'ordinateurs
- Les cartes graphiques (GPU) ont une très grande puissance de calcul et ne sont pas très chères
- Il existe des circuits électronique spécifiquement conçus pour essayer des mots-de-passe (ASICs)

MAIS IL Y A QUAND MÊME DES LIMITES

- Considérons une clé de 128 bit
- 340282366920938463463374607431768211456
- Pour essayer toutes les combinaisons d'une clé de 128 bit pendant une année, les calculateurs consommeraient 30 Gigawatt
- Soit plus de 1% de la consommation mondiale d'énergie !

MAIS IL Y A QUAND MÊME DES LIMITES

Une clé de 128 bits représente déjà une limite impossible à atteindre avec la technologie **actuelle**.

LE CHOIX D'UN BON MOT DE PASSE

LA QUALITÉ DU MOT DE PASSE DÉPEND DE DEUX CARACTÉRISTIQUES:

- La longueur du mot de passe
- Les caractères (l'alphabet) utilisé dans le mot de passe

Le plus important est la longueur du mot de passe

LE CHOIX D'UN BON MOT DE PASSE

POUR UN MOT DE PASSE COMPLEXE (2^128):

- Il faut 22 caractères «complexes» (lettres + chiffres + spécial)
- ou 24 lettres (majuscules + minuscules)
- ou 28 lettres (que des minuscules)

MAUVAIS MOTS DE PASSE

- Les nombres
- Les mots du dictionnaire («seulement» 30'000 - 50'000 mots en Français)
- Les mots du dictionnaires écrits en l'envers
- Les mots du dictionnaire avec un mélange de majuscules et de minuscules (DiCTioNnaIRE)
- Les mots du dictionnaire avec des substitutions simples (D!ct!0nna!r3)
- Noms propres
- Lettres consécutives sur le clavier (qwertzuiop)

LES BONS MOTS DE PASSE

- Mots de passe longs (si possible plus de 20 caractères, mais au minimum 10 caractères)
- Mots de passe avec des caractères quelconques.

VOICI QUELQUES « BONS» MOTS DE PASSE:

X#er/TE4vd@ZvO;S+gS5:wUm
5BT$~Q@e33.0y6-gy,\HHz-i
sJ!Og6B1!lgE<#)HgQb?zv_J
G<L<edZ:eEo<M;+\DX=-{I&]
(G+8cVMdYrx%Ygo3yoT1LS|?>
T3CX6/L2YUYX#1kxV$:go'A"

D'AUTRES BONS MOTS DE PASSE

"GeParrt!ss!peAUneKr!ptaux"
"LaZoliMuzéDHistoyrNatourele"
"Une phrase avec onze mots simples mais ça fait très long"