TD 2 : Mots de passe

1 Choix et évaluation de mots de passe

Question/discussion : Quelle est la taille d'un bon mot de passe ?

Question 1 *Estimez le nombre de mots de passe possibles dans les cas suivants :*

a) le mot de passe est un prénom ;

b) c'est un mot du dictionnaire ;

c) il est composé de quatre chiffres ;

d) il est composé de huit caractères usuels (alphanumériques + spéciaux).

Question 2 *En supposant que le mot de passe est choisi suivant l'un des types précédents, calculez ou estimez le nombre maximal d'essais que l'on peut autoriser pour rentrer un mot de passe si l'on veut limiter la probabilité de succès d'une attaque directe à 2^{-6} ? Et à 2^{-11} ?*

Question 3 *Quel est le temps nécessaire pour mener à bien une telle attaque si on impose un délai d'une seconde après chaque mot de passe faux ? Et si le délai double à chaque mot de passe faux consécutif ? Illustrez ces réponses sur les ordres de grandeurs obtenus à la question précédente.*

Question 4 *Toujours en supposant que le mot de passe est choisi suivant l'un des types précédents, combien de caractères doit-on choisir pour un mot de passe si l'on souhaite une sécurité en 2^{-11}, en 2^{-100}, et en 2^{-128} ?*

Question 5 *Comment doivent-être choisis les mots de passe de la question précédente pour que la garantie de sécurité (i.e. la limite sur la probabilité de succès d'une attaque) soit vraie ?*

2 Haché et salé

Afin d'éviter de stocker les mot de passe en clair sur la machine hôte, on utilise des fonctions de hachage cryptographique. Il s'agit de fonction $H : \{0,1\}^* \to \{0,1\}^n$ qui à toute chaîne m associe une empreinte (un "hash" en anglais, ou haché) $h = H(m)$ de taille fixe (n bits). En outre cette fonction doit vérifier un certain nombre de propriétés telles que la résistance à la première pré-image : étant donné h, trouver un message m tel que $H(m) = h$ doit être difficile (au sens de la complexité algorithmique).

Question 6 *Expliquez comment utiliser une fonction de hachage pour permettre la vérification de mot de passe d'un utilisateur par un serveur sans que le serveur ne stocke les mots de passe. On pourra supposer l'existence d'un canal sécurisé entre l'utilisateur et le serveur pour le transfert du mot de passe.*

Question 7 *Quelqu'un suggère dans ce contexte, que le canal sécurisé n'est plus nécessaire car l'utilisateur n'a plus qu'à transmettre l'empreinte de son mot de passe (qu'il peut calculer lui-même). Pourquoi cela est une mauvaise idée.*

Question 8 *Par recherche en force brute dans un espace de K mots de passe possibles, combien de tentatives sont nécessaires en moyenne pour qu'un attaquant parvienne à pénétrer le système*

a. lorsqu'il connaît une empreinte ?

b. lorsqu'il a récupéré la liste des m empreintes stockées sur le serveur ?

Question 9 *Comparez ce que cela donne en pratique pour des mots de passe choisis selon chacune des options proposées dans la question 1, en supposant que le calcul d'une empreinte prend 1ms et qu'il y a 1000 utilisateurs sur le serveur.*

Pour remédier à ce problème (d'une attaque en utilisant un grand nombre d'empreintes), on utilise une technique dite de salage. Il s'agit de concatener au mot de passe une chaîne aléatoire avant de calculer son empreinte.

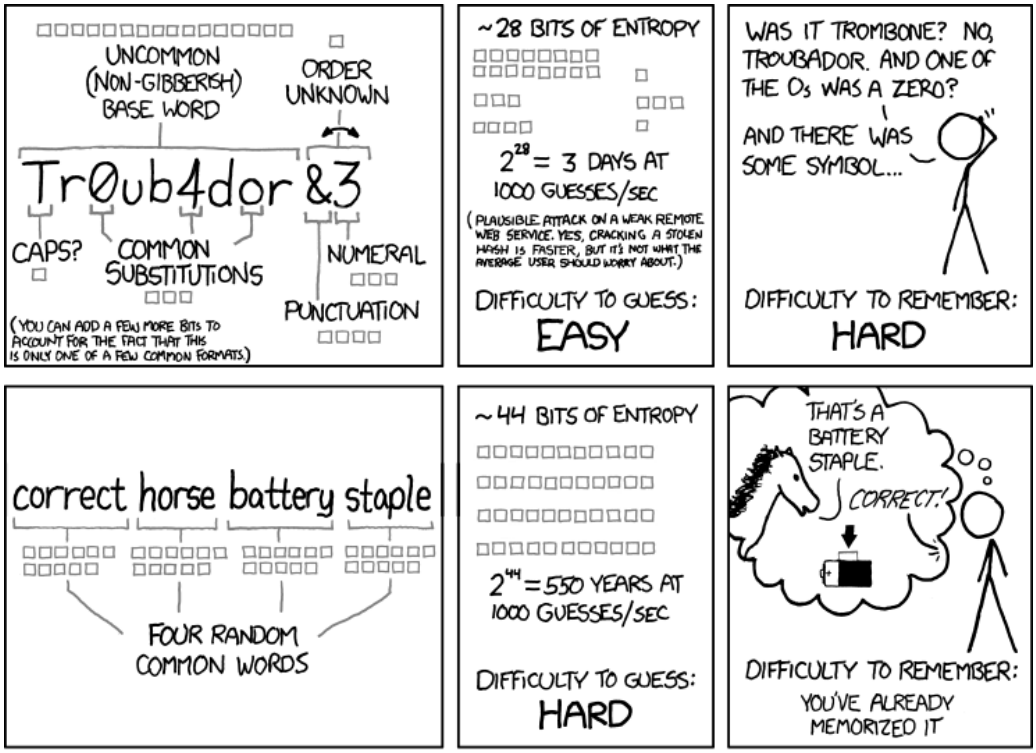
Question 10 *Détailler comment fonctionne désormais le mécanisme d'authentification par mot de passe. En particulier quelles informations sont stockées sur le serveur et quelle information est communiquée de l'utilisateur au serveur.*

Question 11 *Reprendre la question 8 dans le contexte où le salage est introduit.*

Question 12 *Voyez-vous un autre intérêt (ou plusieurs) au salage ?*

3 Password Strength (xkcd 936)

Commentez le webcomic suivant :



Source : R. Monroe, xkcd 936 – *Password Strength* (`https://xkcd.com/936/`)

4 Recommandations NIST

Commentez les recommandations suivantes du NIST (National Institute of Standards and Technology, USA) à propos des mots de passe.

- Longueur minimale : 8 caractères
- Pas de borne supérieure, ou au moins 64 caractères possibles
- Ne pas tronquer les mots de passe
- Pas de règle de composition (contraintes du type : 1 majuscule, 1 minuscule, 1 caractère spécial), mais une liste noire !
- Si un mot de passe est rejeté, expliquer pourquoi, et donner des conseils
- Pas de « question/phrase secrète »
- Pas d'obligation de changer le mot de passe régulièrement (seulement si fuite/attaque → changement obligatoire !)
- Ralentir ou borner le nombre d'essais
- Permettre le copier coller (gestionnaire de mots de passe !)
- Stockage sécurisé (hachage avec sel)
- Utiliser un canal sécurisé (HTTPS, SSH, . . .)