Sécurité informatique

Choix et gestion de mots de passe

Dans le contexte de cette formation, plusieurs restrictions sont imposées lors du choix d'un générateur de mots de passe:

- Génération uniquement via un logiciel (pas d'extensions de navigateur web)
- Logiciels libres uniquement
- Pas de génération de mot de passe sur mobile, uniquement sur PC / laptop
- Idéalement, générer le mot de passe sur un environnement déconnecté, sécuritaire (LiveCD par exemple)

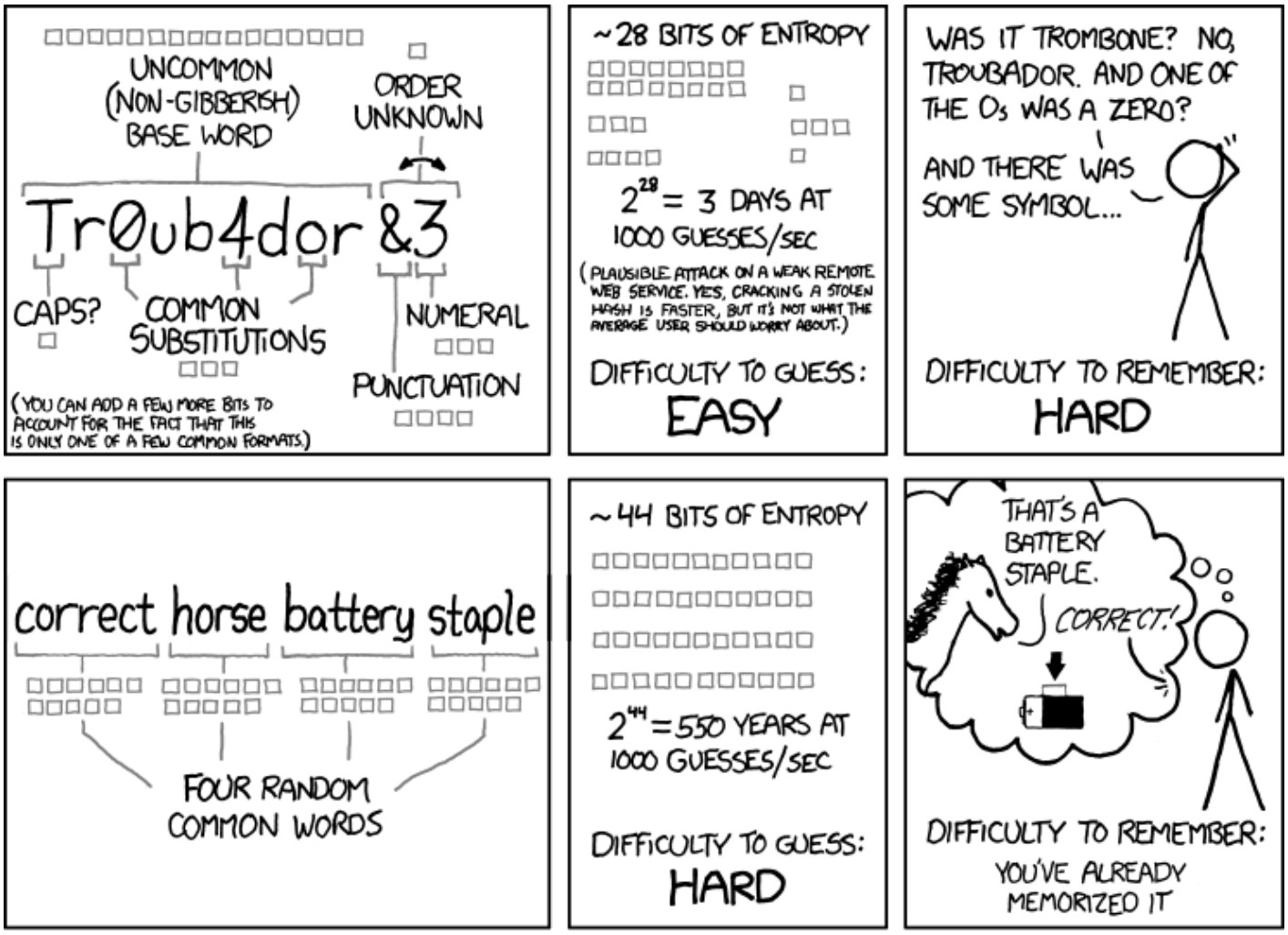
Il est important de tenir compte du modèle de menaces dans le choix de mots de passe. Un bon équilibre entre une gestion commode et des bonne pratiques devraient suffir dans la plupart des scénarios envisagés.

Qu'est ce qu'un bon mot de passe?

Le choix d'un bon mot de passe demeure un des éléments importants lors de la mise en place de mesures de sécurité et protection de renseignements, accès informatiques, etc.

Parmi les bonnes pratiques pour le choix et la gestion de mots de passe on retrouve:

- Le mot de passe peut être prononcé **OU** le mot de passe est impossible à prononcer
- Le mot de passe est “assez long” - ça devient alors une *phrase de passe*
- Il ne contient pas d'informations personelles (ex: date de naissance)
- On ne réutilise jamais le même mot de passe - ceci présume l'utilisation d'un gestionnaire de mot de passe
- On n'a pas à se rappeler et on n'écrit nulle part le mot de passe - présume aussi l'utilisation de gestionnaire de mot de passe
- Connaître et éviter d'utiliser les mots de passe les plus fréquents
- Toujours gardez une bonne copie de sécurité de votre base de données de mots de passe!



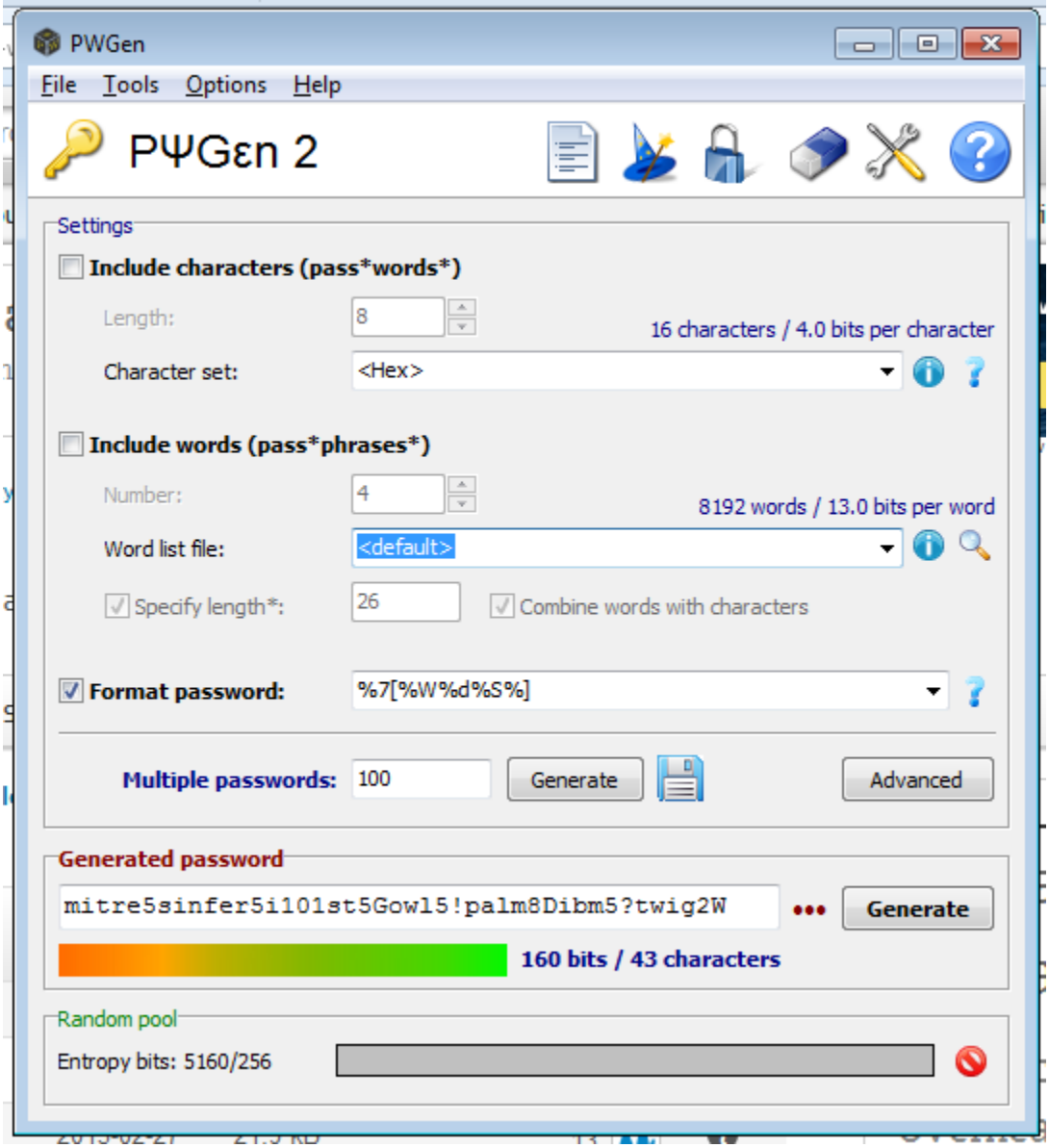
source: XKCD
License Creative Commons Attribution-NonCommercial 2.5

Logiciels générateurs de mots de passe

- Pour Debian, Ubuntu: utiliser l'application en ligne de commande pwqgen disponible via le paquet `passwdqc`:

```
$ pwqgen random=85
permit_time4And2Bombay8sour$
```

- Pour MacOS et Windows, installer PWGen, voici un exemple de paramètre permettant de générer de longs mots de passe (**%7[%W%d%S%]**):



Gestion des mots de passe

KeePass est un gestionnaire de mots de passe publié sous GPL v2 ou ultérieure, qui sauvegarde les mots de passe dans un fichier crypté appelé « base de données »[1]. Cette base est accessible avec le mot de passe principal qu'il faudra choisir avec soin.

Le version suggérée à utiliser est la deuxième (Keepass 2). KeePass s'installe nativement sous Windows, et via la plateforme Mono sous Mac OS, Linux, FreeBSD et autres systèmes d'exploitation.

- Pour Debian, Ubuntu, utiliser:
  - Le paquet `keepass2` utilisant la plateforme Mono si on désire avoir exactement la même version que sur Windows, un accès à de nombreuses extensions, plus de fonctionalités d'import/export et un générateur de mots de passe
  - Le paquet `keepassx` si on ne veut pas installer la plateforme Mono, avoir une meilleure intégration graphique à l'environnement de travail, mais moins de fonctionalités

```
$ sudo apt install keepassx
```

- Pour Windows, téléchargez et utilisez Keepass (version 2.39.1 au moment d'écrire ce texte)
- Pour Mac OS, téléchargez et installez KeepassX. Il est possible d'installer Keepass mais c'est une installation pour utilisateurs expérimentés.
- Sur mobile Android:
  - Installez le gestionnaire d'applications F-Droid proposant la gestion d'installation et mises-à-jour de logiciels libres sur Android.
  - Installez Keepass DX via F-Droid (license GPLv3, dépôt GIT).
- Sur mobile iOS:
  - Installez MiniKeePass à partir du App Store (license GPLv3, dépôt GIT)[2].

Note: sur Android et iOS les applications proposées permettent de débarrer le fichier KDBX via l'empreinte digitale sur des mobile récents via le mécanisme interne d'authentifications d'Android et via TouchID d'Apple, respectivement.

Liens utiles

- https://ssd.eff.org/en/module/creating-strong-passwords
- La méthode Diceware pour générer des mots de passe
- Utilisation de Keepass par plusieurs utilisateurs
- Comment accéder le générateur de mots de passe du système sous Mac OS
- https://securityinabox.org/en/guide/passwords/

1)
https://fr.wikipedia.org/wiki/KeePass
2)
https://www.reddit.com/r/KeePass/comments/818ii1/best_keepass_app_for_iphone/

From:
https://dulib.re/wiki/ - **Le Goût du Libre**

Permanent link:
https://dulib.re/wiki/doku.php/securiteinformatique_motdepasse?rev=1535042172

Last update: **2018/08/23 09:36**