La gestion des mots de passe

Présentation

- Valentin Hubert
  - Animateur TICE *collège école Saint Augustin Angers*

How I became a password cracker

Comment je suis devenu un pirate de mot de passe

- *« Voir son propre mot de passe tomber en moins de quelques secondes est le genre d'expérience que tout le monde devrait faire, ne serait-ce qu'une fois… ne serait-ce que parce qu'elle permet de mieux concevoir ses propres mots de passe »*
- *« On se prend très vite au jeu. […] C'est addictif. C'est comme un puzzle mathématique »*

- Nat Anderson

Mot de passe

- Protéger des données
- Reconnaitre une identité
- Accéder à un contenu protégé

Top 25 des pires mots de passe de l'année 2015

- 123456 (inchangé)
- password (inchangé)
- 12345678 (+1 place)
- qwerty (+1 place)
- 12345 (-2 places)
- 123456789 (inchangé)
- football (+3 places)
- 1234 (-1 place)
- 1234567 (+2 places)
- baseball (-2 places)
- welcome (nouveau)
- 1234567890 (nouveau)
- abc123 (+1 place)
- 111111 (+1 place)
- 1qaz2wsx (nouveau)
- dragon (-7 places)
- master (+2 places)
- monkey (+6 places)
- letmein (-6 places)
- login (nouveau)
- princess (nouveau)
- qwertyuiop (nouveau)
- solo (nouveau)
- passw0rd (nouveau)
- starwars (nouveau)

LinkedIn 117 millions de comptes piratés (24/05/2016)

- En 2012 le site conseil à 6,5 millions d'utilisateurs de changer de mot de passe.
- Longtemps après, une déclaration révèle 100 millions de compte au lieu de 6,5.
- 90% des mots de passe ont été cassés en trois jours.
- LinkedIn conseil d'activer la vérification en deux étapes.

Comment le pirate arrive-t-il à trouver votre mot de passe ?

- L'attaque par brute force (test de combinaison une par une)
  - Très long
  - Dépend de la puissance de la machine
  - De la complexité du mot de passe
- Le Social Engineering (phishing)
  - La personne donne d'elle-même le mot de passe (confiance)
    - EDF – Banque – ami coincé à l'étranger….
  - La sensibilisation est la meilleure arme

Comment le pirate arrive-t-il à trouver votre mot de passe ?

- Les Malwares (Keyloggers)
  - Le hacker reçoit les informations tapées au clavier.
  - Souvent cachés dans des extensions de navigateur, des installateurs de programme…
  - Ne JAMAIS se connecter depuis un ordinateur public sur des sites sensibles.
  - Installer un antivirus et maintenez le à jour.
  - Etre vigilant lors de l'installation de logiciel (installation personnalisée).
    - Télécharger ses programmes sur les sites d'éditeur et non sur des sites de téléchargement (Clubic – 01.net – CommencerCaMarche)

Les caractéristiques d'un « bon » mot de passe

- Sa longueur
  - 10 caractère minimum en 2010
- Sa complexité
  - Aucune logique dans la suite de caractère
  - Non prononçable, non mémorisable
- La variation des caractères utilisés
  - Chiffres, lettres majuscules minuscules, symboles, caractère spéciaux
- Sa durée de vie
  - Il est conseillé de changer ses mots de passe tous les six mois
- Mot de passe à usage unique

?Fe3a/kYuBi4uNduC}/[8a9k4#y6t)[q

- Aucuns être humain ne peut retenir un mot de passe différent ressemblant à celui-ci pour chacun de ses identifiants :

  8;M9:5&@29\pM8<Q!

Un mot de passe pour les retenir tous ?

- Gestionnaire de mots de passe
  - Ils retiennent les mots de passe / identifiants
  - Ils peuvent générer des mots de passe complexe
  - Ils vous indique quand vos mots de passe sont faible.
  - Synchroniser vos mots de passe sur vos différents terminaux
  - Ne retenir qu'un seul « gros » mot de passe
- Dashlane – 1Password – Keepass – Enpass – LastPass – Roboform

Démonstration