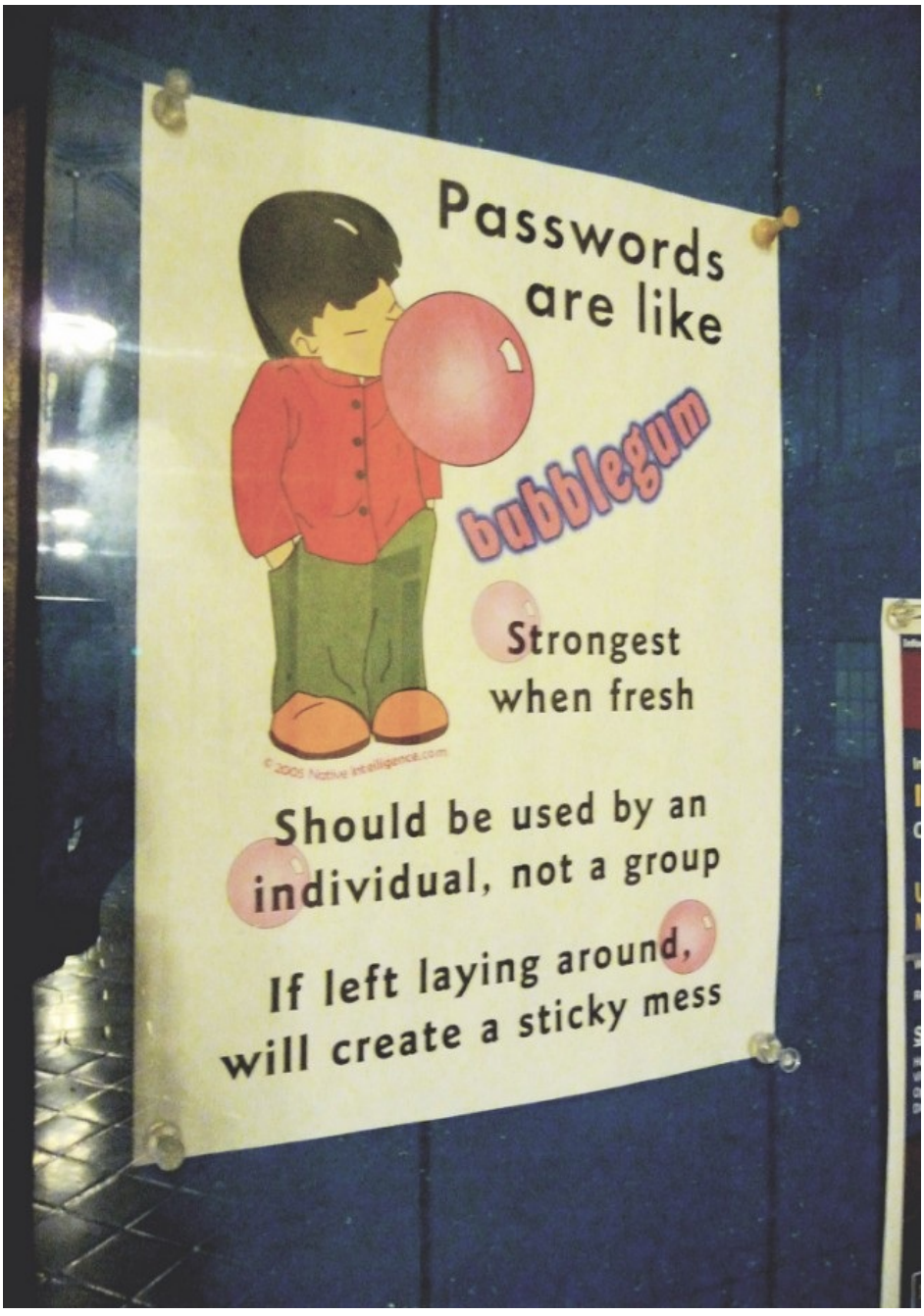
BLINDE TON MOT DE PASSE

LE 14 MAI 2010 ***NICOLAS KAYSER-BRIL***

Le mot de passe est un élément fondamental pour la protection de nos données sur Internet. Quelques conseils et une application pour le choisir au mieux.

Petit test préparé par le **gouvernement US** et trouvé chez **security.tao.ca**

Avez-vous écrit votre mot de passe sur un bout de papier ?
Votre mot de passe est-il un nom commun que l'on peut trouver dans le dictionnaire ?
Votre mot de passe est-il un nom commun suivi de 2 chiffres ?
Votre mot de passe est-il un nom de personne, de lieu ou d'animal ?
Quelqu'un d'autre connait-il votre mot de passe ?
Utilisez-vous le même mot de passe pour plusieurs comptes et depuis longtemps ?
Utilisez-vous le mot de passe par défaut du constructeur ou de l'éditeur ?
Si vous avez répondu oui à l'une des questions ci-dessus (à part la 1 et la 5), vous êtes mal barré ! Un mot de passe simple le rend susceptible à une **attaque par force brute**, où l'assaillant essaye plein de combinaisons rapidement.



Ce type d'attaque n'a que peu de chances de réussir sur un service en ligne, où votre adresse IP sera bloquée au bout d'une dizaine de tentatives et où le temps de réponse du serveur rend cette technique trop longue (là, on préfèrera une attaque d'ingénierie sociale **à**

base de questions de sécurité).
La force brute fonctionne très bien en revanche pour les systèmes où personne ne lit les logs qui enregistrent les tentatives de connexion. C'est le cas par exemple de votre routeur WiFi, dont la clé WEP peut être devinée en quelques minutes.

Pour vous aider à choisir un bon mot de passe, nous avons adapté l'application crée par **smallhadroncollider**, ***How Secure is my Password ?*** Si après ça vous êtres toujours en manque d'imagination, lisez ces conseils pour **choisir un bon mot de passe**.

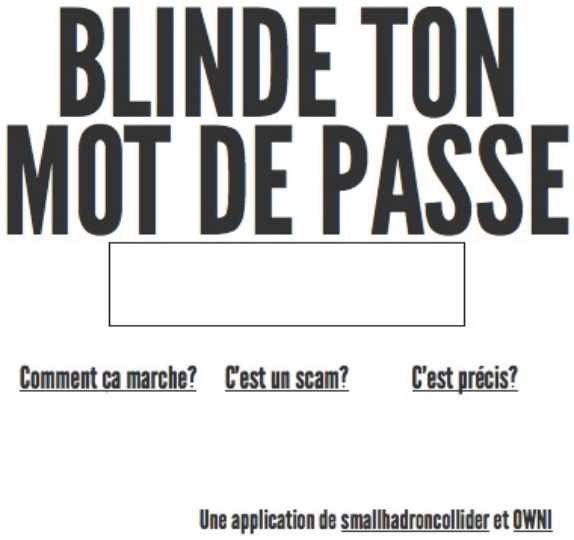


Photo CC ***sponng***

Mise à jour suite au commentaire de Vincent: les questions 1 et 5 ne concernent pas une attaque par force brute.

—

Retrouvez les autres articles de **ce premier volet** de notre série sur le Contre-espionnage informatique : **Des milliers d'emails piratables sur les sites .gouv.fr** et **Enquête : 70 centimes les 1000 captchas**.

Retrouvez également les **deuxième** et **troisième** volets de cette série sur le Contre-espionnage informatique.

MAËLIS
le 14 mai 2010 - 16:05 • SIGNALER UN ABUS - PERMALINK

Hem, donc, si j'ai bien compris, la conclusion de cet article sur la sécurisation des mots de passe, c'est de se rendre sur un site où on donne le mot de passe en question ? Sans autre forme de procès ?
Juste comme ça, pour voir si j'avais bien suivi…

NKB: Comme indiqué sur l'app, tout est en Javascript, si bien qu'aucune donnée n'est stockée nulle part, ni même ne quitte votre ordinateur.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

VINCENT
le 14 mai 2010 - 17:06 • SIGNALER UN ABUS - PERMALINK

Je ne comprend pas bien comment repondre "oui" aux questions 1 et/ou 5 rend le mot de passe plus vulnerable a une attaque par brute force?
De plus, WEP est faible quelque soit la cle utilisee. Meme une cle WEP "blindee" sera decouverte tres rapidement par un voisin disposant des bons outils. Il est necessaire d'utiliser WPA pour prevenir ce genre d'attaques, et la effectivement, il faut bien choisir sa cle.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

SHARE
le 15 mai 2010 - 10:59 • SIGNALER UN ABUS - PERMALINK

Drôle, mais les 500 mots de passe automatiquement considérés comme pas sûr sont anglo-centrés (voir le code source de la page). “Password” est marqué comme crackable instantanément mais “Motdepasse” est présenté comme sûr.

Deux liens pas inutiles pour compléter :

http://rumkin.com/tools/password/passchk.php

http://www.passwordmeter.com/

NKB: J’ai cherché pendant près d’une heure une liste des mots de passes les plus fréquents en français, sans succès. Si vous savez où trouver ça, ou bien où trouver le dump d’une base de données avec 10000+ mots de passes, on aura fait avancer les choses!

En attendant, j’ai mis à jour le Javascript.

Si vous avez d’autres mots de passes ultra fréquents, n’hésitez pas à les balancer ici, je mettrai à jour au fur et à mesure.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

NARDINO
le 16 mai 2010 - 22:20 • SIGNALER UN ABUS - PERMALINK

Bizarre que :
aaaaaaaaaaa
Nécessite 302 jours
Alors qu’un truc du genre :
n0r3tl,z
Se trouve en 38 jours.

La longueur du mdp serait-elle un obstacle suffisant ?

NKB: Merci pour la remarque. Effectivement, un mot de passe avec une seule lettre répétée risque d’être trouvé plus facilement qu’un mot de passe comportant des majuscules, des caractères spéciaux et des chiffres. Maintenant, l’algo derrière l’app ne fait que compter le nombre de possibilités différentes en fonction des caractères utilisés, en faisant tout simplement (nombre de caractères possibles)^(longueur du mdp). Là avec 12 minuscules ça donne 26^12 = 9e16 possibilités contre 75^8 = 1e15 possibilités dans l’autre cas.

Promis si on fait une V2 de l’app on prendra en compte les cas particuliers!

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

DEHKS
le 19 mai 2010 - 6:25 • SIGNALER UN ABUS - PERMALINK

Plus c’est long, plus c’est long…

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

DEHKS
le 19 mai 2010 - 6:48 • SIGNALER UN ABUS - PERMALINK

j’ai oublié de préciser que mon mail n’existe pas.
Pourquoi mail required si on peut mettre n’importe quoi?

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

MARTACHAN

le 21 mai 2010 - 16:13 • SIGNALER UN ABUS - PERMALINK

When you're in a not good position and have got no money to move out from that point, you will need to receive the personal loans. Just because that would help you for sure. I get secured loan every year and feel great because of this.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

JOE
le 16 juillet 2010 - 15:03 • SIGNALER UN ABUS - PERMALINK

Il manque une question sur la taille du mot de passe, en général j'utilise un mot de passe de 9 caractères la moulinette estime 237 ans de calculs pour celui-ci … Je l'utilise souvent certes, mais il reste assez sûr tout de même ;)

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

FLORENT
le 16 juillet 2010 - 19:00 • SIGNALER UN ABUS - PERMALINK

WEP a de grosses failles au niveau cryptographique. Cracker une clef WEP rapidement demande l'exploitation de ces failles (qui sont décrites en détail dans de nombreux white paper), ce qui n'est en rien comparable à une attaque par force brute.

C'est dans le cas du WPA, chiffrement ne souffrant d'aucune faille exploitable actuellement, que l'on est obligés d'utiliser la force brute (et encore – pour peu que le SSID soit relativement commun, on peut utiliser des rainbow tables).

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

TOTO
le 1 novembre 2011 - 21:51 • SIGNALER UN ABUS - PERMALINK

Il faudrait par contre préciser la puissance de l'ordinateur qui est prit comme repère pour le calcul.

VOUS AIMEZ 0 VOUS N'AIMEZ PAS 0 LUI RÉPONDRE

3 pings

Les tweets qui mentionnent Blinde ton mot de passe » Article » owni.fr, digital journalism -- Topsy.com le 14 mai 2010 - 16:29

[...] Ce billet était mentionné sur Twitter par Nicolas Voisin, Aurélien Fache, Maëlis Jamin-Bizet, Owni, Likiwi et des autres. Likiwi a dit: RT @0wn1: [#owni] Blinde ton mot de passe http://bit.ly/b2FL5q [...]

Les tweets qui mentionnent Blinde ton mot de passe ! -- Topsy.com le 16 mai 2010 - 18:06

[...] Ce billet était mentionné sur Twitter par micmac. micmac a dit: Blinde ton mot de passe ! http://twurl.nl/cv5kmz [...]

Des milliers d'emails piratables sur les sites .gouv.fr » Article » OWNI, Digital Journalism le 24 septembre 2010 - 18:28

[...] Blinde ton mot de passeLa Fabrique du Data #2Enquête: 70 centimes les 1000 captchasLâche ton poncifLe web est-il mort ? / Is the web dead ?Fermeture imminenteAudience web et classement : attention aux noms des tableaux mediametriePACinfo: Où sont passés les 10 milliards de la PAC?Presse en ligne: qui

touche les subventions?Politiques et numérique… [...]