

□□□□□□□□□□□□□□□□□□  
 Mot de base inhabituel  
 (mais pas du charabia)

□  
 ordre  
 inconnu

Tr0ub4dor &3

maj.? □  
 confusion possible □□□  
 chiffres □□□  
 ponctuation □□□□

~ 28 bits d'entropie

□□□□□□□□ □  
 □□□□□□□□ □  
 □□□ □□□  
 □□□□ □

$2^{28} = 3$  jours à raison  
 de 1000 tests / sec.

Attaque plausible sur un service  
 web peu performant.

Difficulté à «craquer»  
**FACILE**

Est-ce que c'était  
 «trombone» ?  
 «Troubadour» ?  
 L'un des O était  
 un 0 ?  
 Y avait-il un  
 symbole ?

Difficulté à retenir  
**DIFFICILE**

correct cheval agraffe pile

□□□□□□ □□□□□□ □□□□□□ □□□□□□  
 □□□□□□ □□□□□□ □□□□□□ □□□□□□

4 noms communs  
 pris au hasard

~ 44 bits d'entropie

□□□□□□□□□□ □□□□□□□□□□  
 □□□□□□□□□□ □□□□□□□□□□  
 □□□□□□□□□□ □□□□□□□□□□  
 □□□□□□□□□□ □□□□□□□□□□

$2^{44} = 550$  ans à raison  
 de 1000 tests / sec.

Difficulté à «craquer»  
**DIFFICILE**

C'est une  
 agraffe sur  
 une pile.

Correct !

Difficulté à retenir  
**Déjà mémorisé !**

En 20 ans d'effort, nous avons réussi à faire en sorte que tout le monde utilise des mots de passe difficile à mémoriser pour l'homme, mais facile à «craquer» pour un ordinateur.