Attaques par mots de passe

CNEJITA - 2 février 2016

Attaque par mot de passe: préalables

@ **Pour pouvoir « essayer » un mot de passe, il faut maîtriser :**

- la fonction de dérivation de mots de passe
- la fonction de vérification des mots de passe.

@ Ce sont sur ces deux fonctions que repose la sécurité des logiciels, elles vont déterminer la performance des crackers.

Dérivation du mot de passe

Fonction de dérivation : « passage de l'utilisateur à la machine »

@ Les fonctions simples de type : dk = hash(password)

@ Les fonctions standard : PKCS#5
Le but de ce type de fonctions, de plus en plus courantes, est de rendre les attaques par essais successifs lentes

- PBKDF2 (RFC 2898) :

DK = PBKDF2(PRF, Password, Salt, c, Dklength)

- SCRYPT : fonction alternative à la précédente qui prévient l'utilisation de GPU.

Liberté · Égalité · Fraternité
RÉPUBLIQUE FRANÇAISE
Centre Technique d'Assistance

Vérification d'un mot de passe

- **Vérification de type comparaison de hash :**
  - Dérivation du mot de passe à tester
  - Comparaison avec le hash stocké

- **Vérification de type « déchiffrement »:**
  - Dérivation du mot de passe
  - Déchiffrement d'une partie du fichier chiffré (ex. entête)
  - Vérification des données déchiffrées (CRC, magic, …)

Centre Technique d'Assistance

Attaques par force brute

Force brute : tenter successivement un ensemble de mots de passe

@ Attaques exhaustives ?
- Sur les clefs de chiffrement … !
- Sur les mots de passe … dans les bons cas !

@ Paramètres des attaques :
- Choix du jeu de caractères (charset)
- Choix de la longueur des mots de passe à tester

Nombres de mots passe à tester = (taille du charset)$^{longueur\ du\ mot}$

Liberté · Égalité · Fraternité
RÉPUBLIQUE FRANÇAISE
Centre Technique d'Assistance

Optimisations

1. Tables rainbow
2. Chaînes de Markov
3. Cryptanalyse
4. Dictionnaires

Tables Rainbow (1)

- Compromis temps/mémoire *: l'attaque repose sur une table de précalculs permettant d'accélérer la recherche d'un mot de passe sans avoir à stocker l'intégralité des empreintes de mots de passes.*

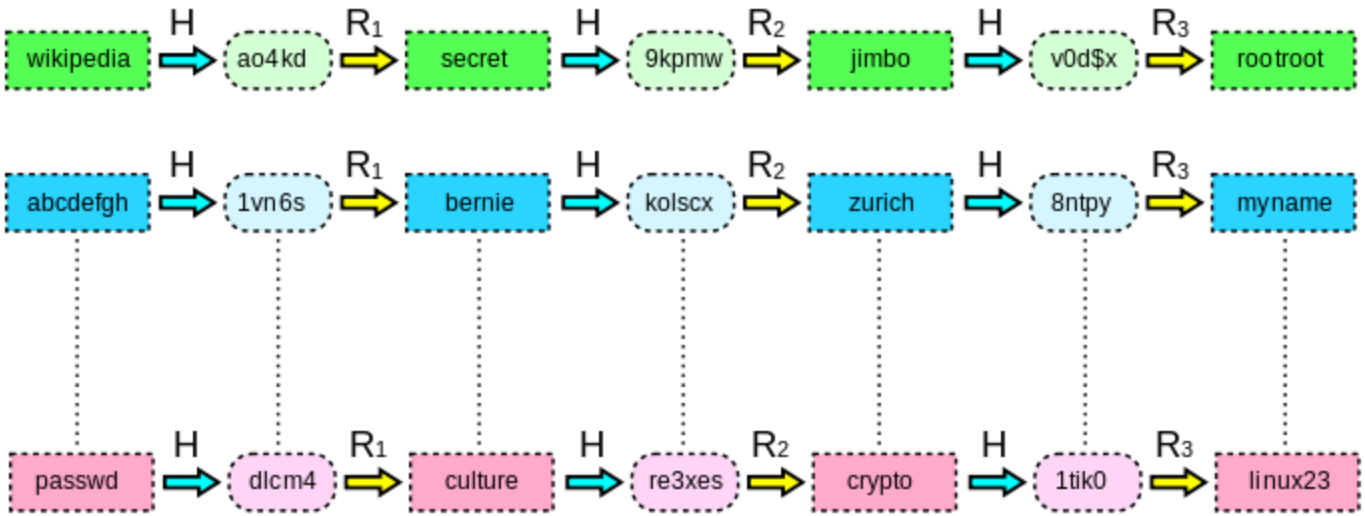
- *Avantages :*
  - *Maîtrise du taux de réussite (choix des paramètres de l'attaque)*
  - *Rapidité des attaques*

- *Inconvénients :*
  - *Coût initial en calcul*
  - *Les cas d'usage sont limités (sel)*

Centre Technique d'Assistance

Tables Rainbow (2)

Exemple de table Rainbow (wikipedia)



Chaînes de Markov et méthodes statistiques

- L'idée est de générer « arbitrairement » des mots qui ressemblent à des « vrais » mots.

  Cela permet d'éviter de tester des mots de passe « improbables ».

Cryptanalyse

Trouver un biais dans la dérivation du mot de passe :

- Fonction pseudo-aléatoire suffisamment prédictible
- Fonction inversible
- Espace des clefs générées trop faible
- Collisions dans les mots de passe / mots de passe équivalents
- …

Liberté · Égalité · Fraternité
RÉPUBLIQUE FRANÇAISE
Centre Technique d'Assistance

Dictionnaires

Limiter l'espace des mots de passe à un ensemble limité qui a un « sens »

Cf. partie suivante !

Paramètres des dictionnaires

- En fonction du produit attaqué :
  - Langue : encodage des caractères, comportement du logiciel selon la langue de saisie.
  - Longueur des mots : ni trop petite, ni trop grande
  - Nombre de mots

Centre Technique d'Assistance

Choix des dictionnaires (1)

- Sur « étagère » :
  - Payants
  - Bases de mots de passe issues de piratages
  - Dictionnaires des outils de traduction
  - Dictionnaires de citations
  - Dictionnaires de titres de livres
  - Indexations diverses et variées (wikipedia, …)
  - …

Centre Technique d'Assistance

Choix des dictionnaires (2)

@DIY :

- Indexations des supports (plusieurs méthodes)
- Les tableaux de chasse : tous les mots de passe connus dans l'affaire (mots de passe « simples » à récupérer : navigateurs web, mots de passe de session, …)
- Les personnalisés : étude de l'environnement
  - Analyse du contenu des documents pour essayer de trouver un champ lexical
  - Compilation sociale de l'utilisateur : prénoms, dates et lieu de naissances, …

Liberté · Égalité · Fraternité
RÉPUBLIQUE FRANÇAISE
Centre Technique d'Assistance

Diversification des dictionnaires (1)

- Les règles du type « John the Ripper »
  - Inversion de mots
  - Ajout, suppression de caractères
  - Concaténation (devant, derrière)
  - Changement de casse
  - …
  - Combinaisons de règles

Attention au nombre de mots générés en sortie !

Centre Technique d'Assistance

Diversification des dictionnaires (2)

- Combinaison de dictionnaires

- Attaques hybrides : force brute et dictionnaire

Les outils commerciaux ne sont pas toujours très fournis ni très personnalisable.

Dernière optimisation

@La question : **article 434-15-2**

3 ans d'emprisonnement et 45000€ en cas de non divulgation du mot de passe

Liberté · Égalité · Fraternité
RÉPUBLIQUE FRANÇAISE
Centre Technique d'Assistance

Des questions ?

francois.delost@interieur.gouv.fr

01.47.48.07.74