Choix du chiffrement des mots de passe

1. Choix retenus / étudiés

- MD5
- SHA-1 + Salt
- bcrypt

2. Description technique

2.1 MD5

- 128-bit/16-byte digest
- plus rapide
- exemple : actuellement il est possible de calculer un hash MD5 de 6 caractères composé d'alphanumériques en minuscule en 40 secondes.

2.2 SHA-1 + Salt

- 160-bit/20-byte digest
- meilleure résistance aux attaques par brute force

2.3 MD5/SHA-1/SHA-256/SHA-512/SHA-3

- fonction de hachage a usage général
- conçu pour calculer de grosses quantités de données le plus rapidement possible
- faible résistance face aux attaques par rainbow table (en raison d'une montée en puissance des avancées de calcul)

2.4 bcrypt

- variante de l'algorithme de Blowfish
- utilise un Salt
- utilise un facteur de travail (permettant de gérer la balance entre rapidité et robustesse)

3. Solution retenue

Aucuns des algorithmes « standard » n'est retenu étant donné leur faible robustesse face aux puissances de calculs des GPUs et des supercalculateurs actuels.

Cependant, bcrypt reste résistant face aux attaques par brute force et par rainbow table.

En effet il est basé sur l'algorithme de chiffrement Blowfish et implémente en plus un Salt et un facteur de travail ce qui permet de gérer le nombre d'itération de calcul et donc de temps de chiffrage.

Plus le facteur de travail est élevé, plus les attaques nécessitent de temps et de puissance de calcul.

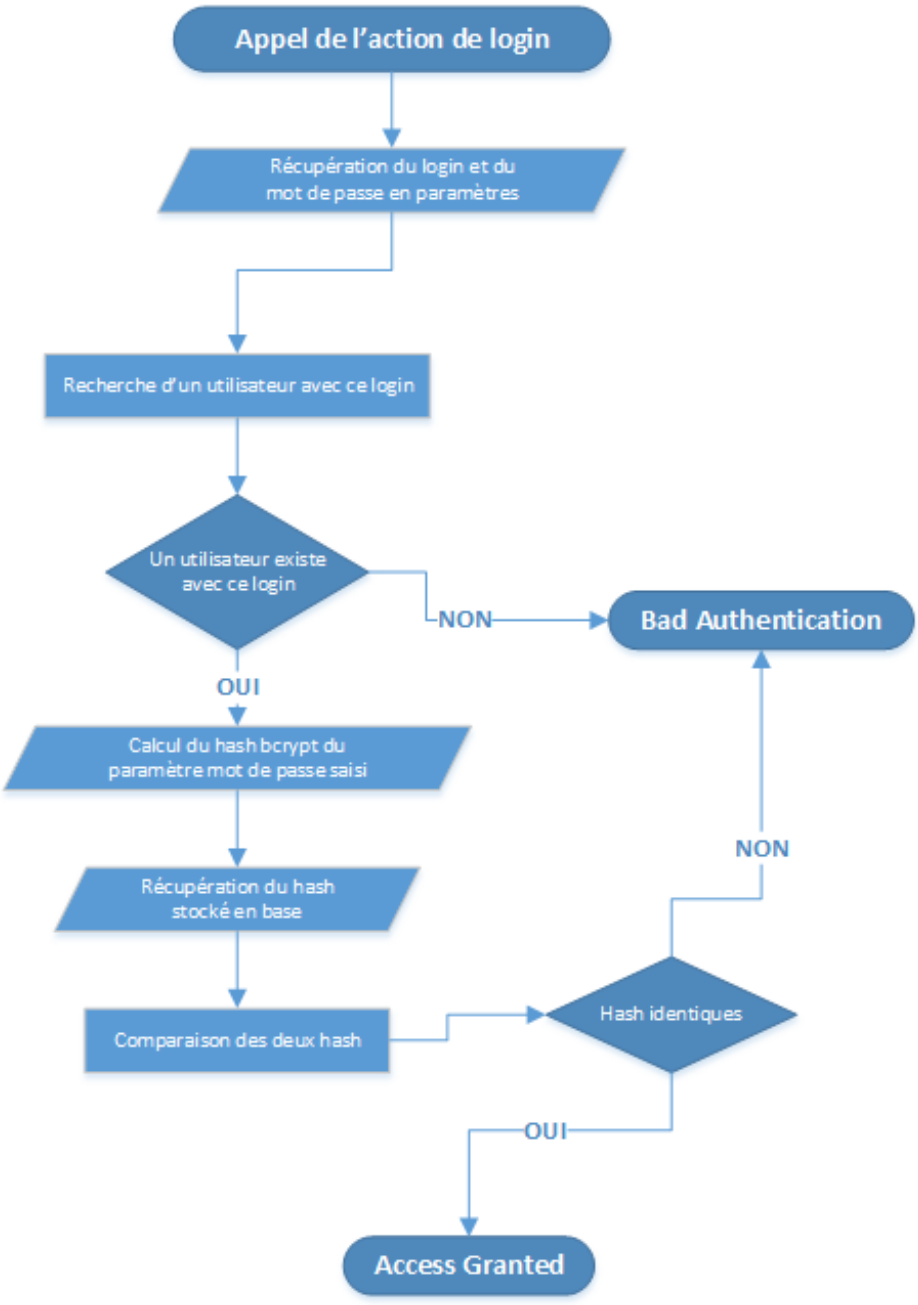
Par exemple, pour un facteur de travail de 12, bcrypt chiffre le mot de passe « yaaa » en environ 0,3 secondes alors que MD5 le fait en moins d'une micro seconde.

4. Impacts/Modifications techniques sur les applications actuelles

4.1 Base de donnée

- Modification du champ utimdp de la table utilisateur => CHAR(60) au lieu de VARCHAR(32)

4.2 Process de login



(* : Facteur de travail fixé à 12 par défaut)

4.3 Modèles, Mappeurs, Classes, Contrôleurs, Plugins

- Modification du modèle utilisateur dans livrable 2 pour le type de champ utimdp
- Modification de la gestion des ACLs pour l'implémentation du nouveau process de login (création d'un plugin de Zend_Auth) pour le livrable 1