3TI
Sécurité des réseaux informatiques
2015-2016

Authentification de l'utilisateur

V.Van den Schrieck

Brainstorming

Par groupes de 3 étudiants :

- C'est quoi, l'authentification de l'utilisateur?
- Comment peut-on authentifier un utilisateur?

Temps imparti : 10 minutes

L'authentification

Deux étapes :

1. **L'identification**
2. **La vérification**

http://en.memory-alpha.org/wiki/File:Identification_card,_Christine_Chapel.jpg

Système d'authentification

Pour authentifier un utilisateur, il doit être **connu** du système

- Phase d'enregistrement
- Stockage d'un élément caractéristique permettant l'authentification
  - Connu par l'utilisateur (mot de passe)
  - Possédé par l'utilisateur (token)
  - Caractérisant l'utilisateur (biométrie)
  - Fait par l'utilisateur (parole, écriture, frappe au clavier, …)

Authentification par mot de passe

Discussion en groupes de 3 : Sur base du TP de la semaine passée,

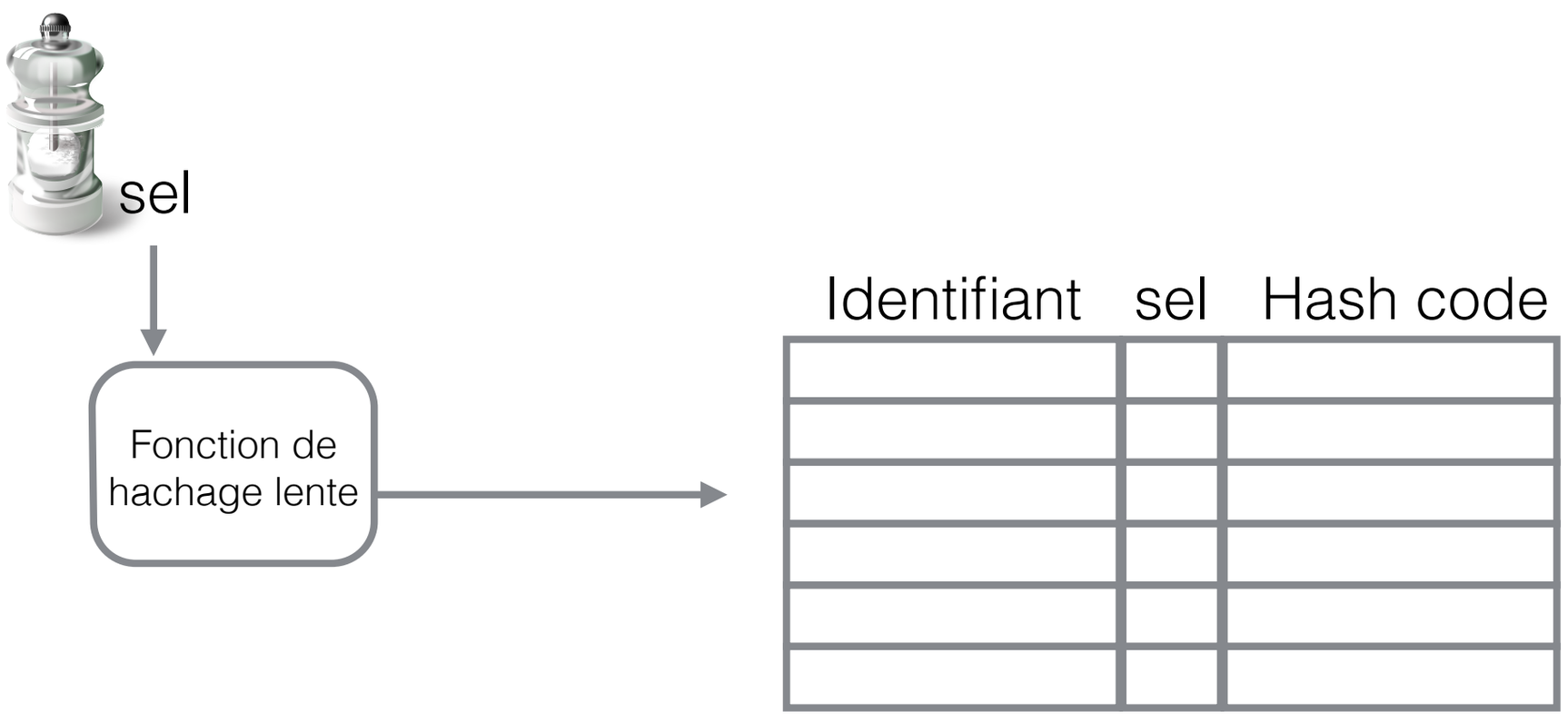
- Expliquez les vulnérabilités observées au niveau des mots de passe
- Proposez des contre-mesures pour augmenter la sécurité de l'authentification par mots de passe

Temps imparti : 10-15 minutes

Attaques sur les mots de passe

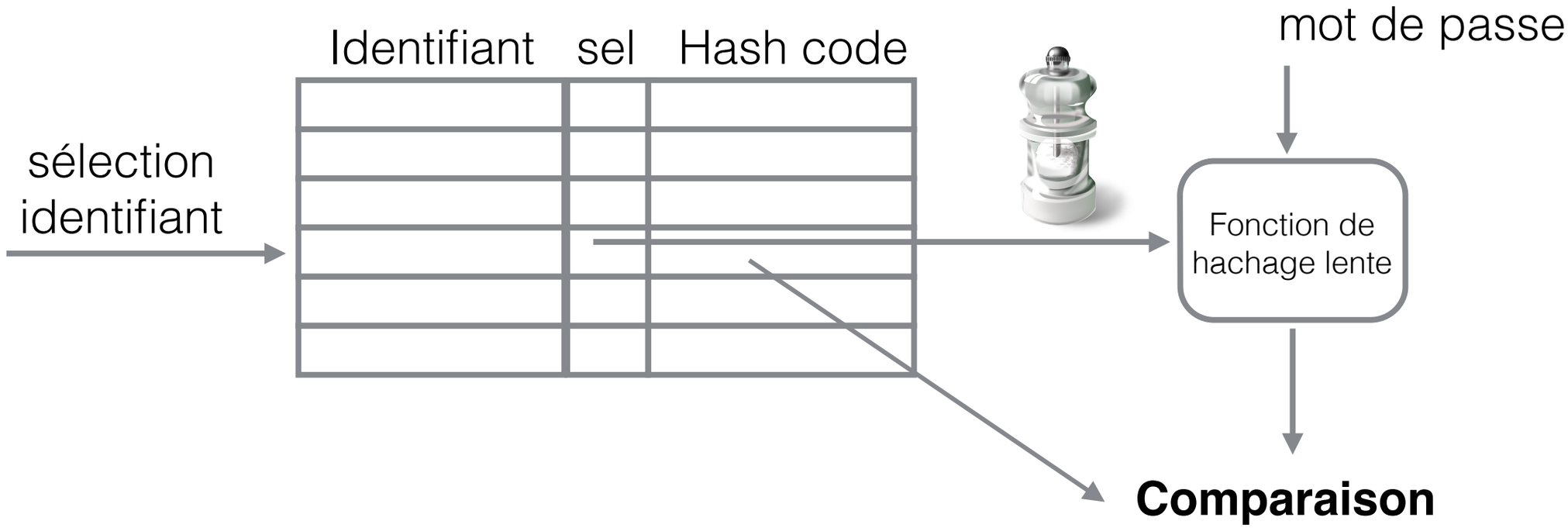
- Dictionnaire hors ligne
- Mots de passe populaires
- Cible spécifique
- Piratage de poste de travail
- Social engineering
- Usage multiple de mots de passe
- Surveillance électronique

Mots de passe hachés



Stockage d'un mot de passe en UNIX

Mots de passe hachés



Vérification d'un mot de passe en UNIX

Objectifs du sel

1. Masquage des mots de passe identiques dans un fichier (sels différents)
2. Attaque par dictionnaire complexifiée
3. Masquage de l'utilisation de mots de passe identiques sur plusieurs machines

Craquage de mots de passe

http://fr.wikipedia.org/wiki/Grand_dictionnaire_universel_du_XIXe_siècle#mediaviewer/File:Grand_Larousse_du_XIXe_siècle_(2).JPG

http://pixabay.com/fr/arc-en-ciel-couleurs-belle-vives-33149/

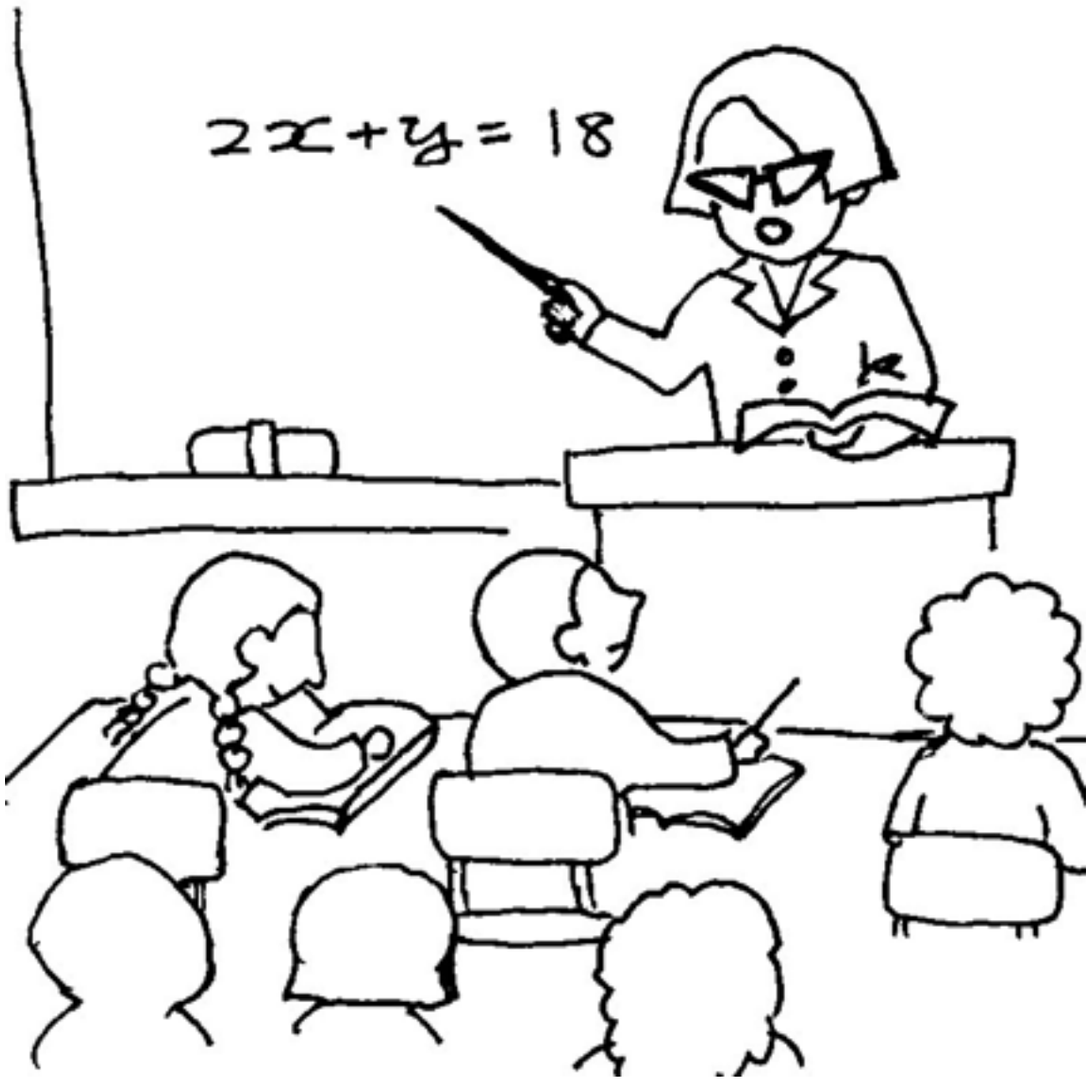
https://ru.wikipedia.org/wiki/ТАРДИС

http://pixabay.com/fr/disque-dur-technologie-de-stockage-42935/

Sécurité du fichier de mots de passe

http://www.paranormalhaze.com/img/mistery/shadow-people/shadow-people04.jpg

Sécurité des mots de passe

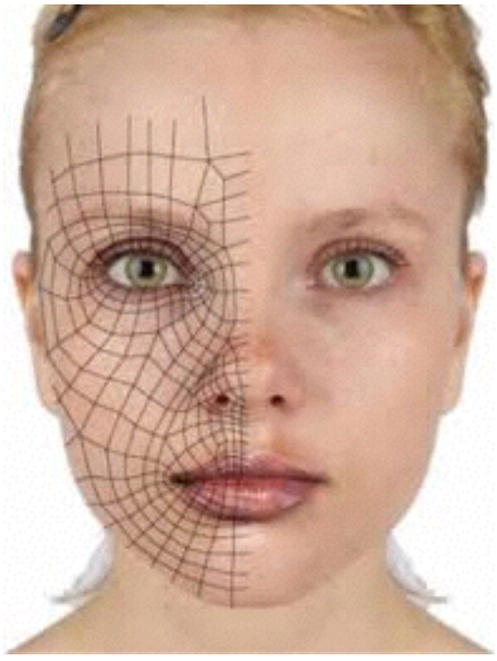


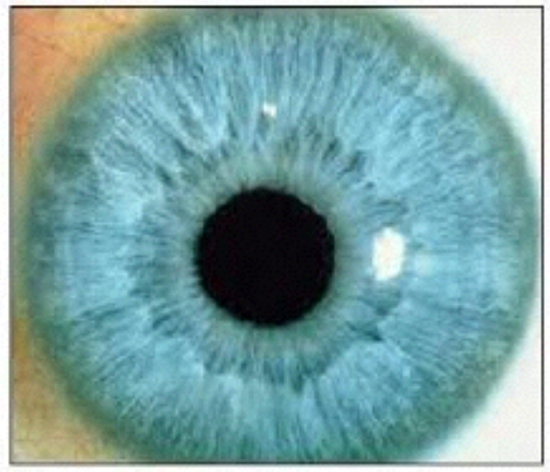
Sécurité des mots de passe

Sécurité des mots de passe

Authentification par token

Authentification par biométrie





Authentification par biométrie

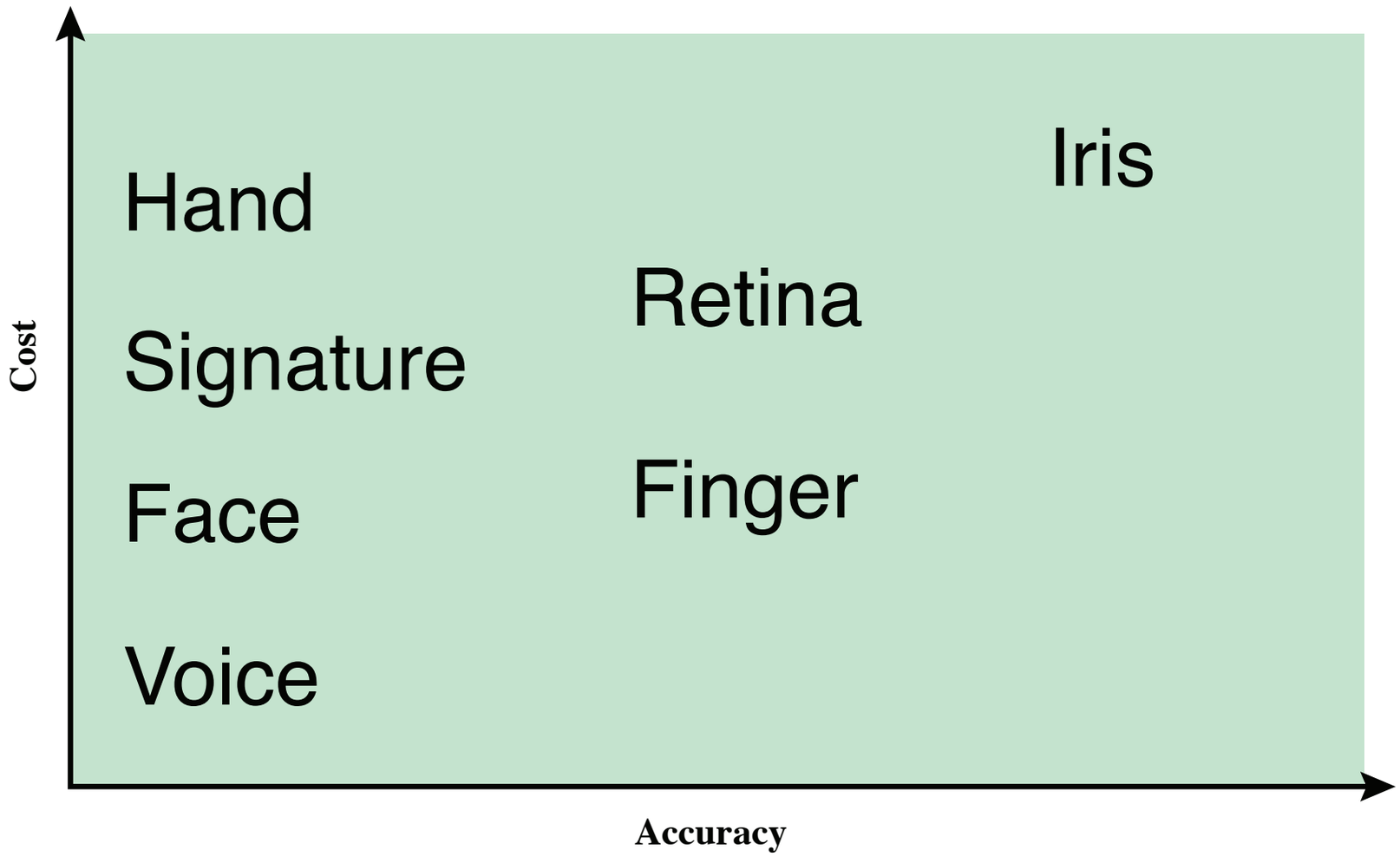


Figure 3.7 Cost Versus Accuracy of Various Biometric Characteristics in User Authentication Schemes.

Source : Stallings

Authentification à distance

http://upload.wikimedia.org/wikipedia/commons/thumb/f/f6/Théodore_Jacques_Ralli_Eavesdropping_1880.jpg/701px-Théodore_Jacques_Ralli_Eavesdropping_1880.jpg

Risque supplémentaire : **l'écoute**

=> Capture du mot de passe

=> Rejeu

Solution :

Challenge/réponse

Attaques sur l'authentification

- Attaques Client
- Attaques Hôte
- L'écoute
- Le rejet
- Cheval de Troie/Phishing
- Déni de service

Pour la semaine prochaine

- Lectures :
  - Syllabus
  - Belgian eID (Campus Virtuel)
- Intervenante extérieur : Mme Wendy Brévière