TD2– Authentification Biométrique

QCM

1. Quelle différence y a-t-il entre identification et authentification ?
   a) Identification = 1:1 ; Authentification = 1:N
   b) Identification = 1:N ; Authentification = 1:1
   c) Les deux sont équivalentes
   d) L'authentification est toujours biométrique
2. Quel type de biométrie est considéré comme **comportementale** ?
   a) Empreinte digitale
   b) Voix
   c) Iris
   d) Forme de la main
3. Que signifie EER ?
   a) Évaluation des erreurs résiduelles
   b) Erreur d'égalité en reconnaissance
   c) Taux d'erreur égal
   d) Aucun des choix
4. Une propriété importante d'un bon système biométrique est :
   a) Sa vitesse d'installation
   b) Son universalité
   c) Sa connectivité
   d) Le nombre de pixels utilisés
5. Le spoofing consiste à :
   a) Réinitialiser les mots de passe
   b) Forcer un utilisateur à poser son doigt
   c) Tromper le capteur avec une fausse donnée
   d) Supprimer une base de données biométrique
6. L'attaque par injection consiste à :
   a) Modifier le capteur
   b) Insérer une image falsifiée dans le système
   c) Changer la base de données
   d) Aucune de ces réponses
7. Le FAR désigne :
   a) Taux de faux rejets
   b) Taux de vrais positifs
   c) Taux d'acceptation des imposteurs
   d) Taux de reconnaissance moyenne
8. Au Burkina Faso, l'organisme chargé des données personnelles est :
   a) CIL
   b) RGPD
   c) APDP
   d) ARCEP
9. La reconnaissance faciale est problématique car :
   a) Elle est lente
   b) Elle n'est pas fiable sur les enfants
   c) Elle peut violer la vie privée
   d) Elle coûte très cher
10. Le chiffrement des gabarits sert à :
    a) Accélérer la reconnaissance
    b) Réduire les coûts de stockage

c) Protéger les données biométriques
d) Améliorer l'image du capteur

Questions de cours

1. Expliquez la différence entre les biométries **physiques** et **comportementales**, avec deux exemples pour chaque.
2. Quelles sont les six principales **caractéristiques** attendues d'un système biométrique fiable ?
3. Décrivez brièvement les étapes d'un **système biométrique complet**, du capteur à la décision finale.
4. Pourquoi les données biométriques sont-elles classées comme **données sensibles** par le RGPD et la loi burkinabè ?
5. Que sont les **attaques par reconstruction** et quels sont les risques qu'elles posent ?

Exercices

Exercice 1

Un lycée privé veut installer un **système de reconnaissance faciale** pour gérer la présence des élèves.
Vous êtes consultant en cybersécurité. Donnez :

- Les **avantages** techniques du dispositif
- Les **risques éthiques** et juridiques
- Vos **recommandations**

Exercice 2

Évaluez le système suivant selon les critères : universalité, permanence, collectabilité, performance, acceptabilité, résistance à la fraude.

Critère	Empreinte	Reconnaissance faciale	Voix
Universalité			
Permanence			
Collectabilité			
Performance			
Acceptabilité			
Résistance			

Exercice 3

Un hacker a récupéré les **modèles biométriques** stockés sans chiffrement dans une base SQL.

Proposez une **mesure technique** et une **mesure organisationnelle** pour éviter ce type de fuite à l'avenir.