Authentification des usagers

- Par quelque chose qu'il connaît
  - mot de passe
  - phrase de passe
  - information personnelle
    - nom
    - date de naissance
    - No. d'ass. sociale
    - …
- Par quelque chose qu'il possède
  - carte magnétique
  - carte à puce
  - « dongle »
  - dispositif « Secure ID"
  - dispositif ou carte RFID
- Par quelque chose qu'il est (biométrie statique)
  - empreintes digitales
  - géométrie de la main
  - rétine de l'œil
  - iris de l'œil
  - caractéristiques du visage
- Par quelque chose qu'il fait (biométrie dynamique)
  - signature
  - voix
  - rythme au clavier
  - géolocalisation

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Authentification par possession d'un objet unique

- Doit être vraiment unique
- Doit être difficile/coûteux à reproduire
- Possiblement indépendant d'une base de données
- Problème de gestion de ces objets
  - émission
  - contrôle de possession
  - perte ou vol
  - récupération
- Faiblesses
  - coût
  - possibilité de falsification
  - perte ou vol
- Cas particulier
  - Ré-authentification
  - détection de la présence continue de l'usager

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

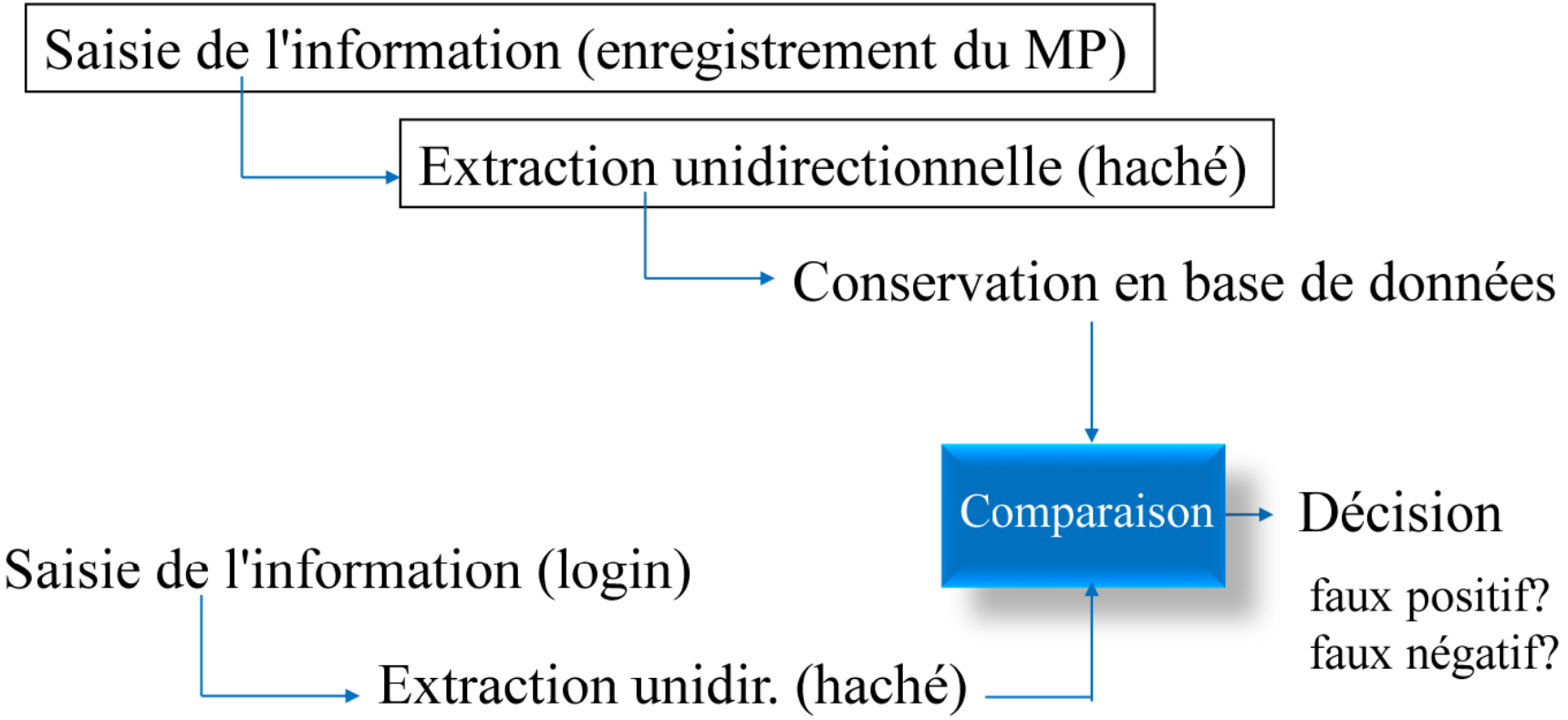
Authentification biométrique statique

- Empreintes digitales
  - bonne précision: expérience policière antérieure
  - la contrefaçon est possible
- Géométrie de la main
  - assez précise
  - contrefaçon ?
- Rétine de l'œil
  - la plus précise des méthodes biométriques
  - utilisation d'un laser : réticence des usagers
  - peut être affectée en cas de maladie de l'usager
- Iris de l'œil
  - très précise :
    - 266 caractéristiques => 10^{78} combinaisons
  - lecture jusqu'à un mètre
  - n'est pas affecté par l'Age, la maladie incluant la cataracte
- Caractéristiques du visage
  - se rapproche le plus de la méthode humaine
  - le taux de précision reste à améliorer
  - utilisé pour identifier des individus dans des lieux public

Authentification biométrique dynamique

- Signature
  - tient compte de la dynamique du geste et non seulement de l'apparence de la signature
  - il faut entrainer le système: décision « floue »
  - la décision est sous forme d'une probabilité
- Voix
  - le moins précis de toutes ces méthodes biométriques
  - il faut entrainer le système
  - sensible à l'état de santé de la personne (laryngite)
  - contrefaçon facile
  - très accepté en général
- Rythme au clavier
  - pas encore très développé
  - décision « floue »
  - complètement transparent pour l'usager
  - surveillance continuelle tant que le clavier est utilisé
  - non-applicable si une interface graphique d'usager est utilisée

Authentification par mot de passe - modèle général



Attaque sur les mots de passe

- Techniques de base
  - Capturer et lire le fichier des mots de passe
    - surtout s'il n'est pas haché
  - Deviner le mot de passe
    - Online/Offline
  - Capturer le mot de passe
    - Enregistreurs de touches (« keyloggers »)
    - Post-it
    - Regard indiscret (« Shoulder-surfing »)
  - Demander à l'usager
    - à son insu
      - Ingénierie sociale (« Social engineering »)
      - Supplantation
    - avec sa collaboration
      - $$$
      - « Talents »

Attaque sur les mots de passe

- Vulnérabilités de mots de passe
  - mots de passe probables
    - mots de passe courts
    - mots du dictionnaire
  - mots de passe avec lien à l'usager
    - information personnelle
    - information familiale

  (Problème de base : faible entropie des choix de mots de passe !!!)
  - mauvaise protection des fichiers de mots de passe
  - pas d'authentification du système

Attaques sur les mots de passe

Capturer le fichier des mots de passe hachés (attaque dictionnaire)

1. Construire une liste de mots de passe possible, $w_1 \ldots w_t$
2. Pour chaque w_j, calculer $h_j=H(w_j)$ et stocker dans une table T les paires (h_j,w_j), trier par h_j
3. Voler une base données de mots de passe hachés $h_i=H(p_i)$
4. Chercher le mot de passe p_i correspondant a l'utilisateur u_i avec hash h_i en cherchant si h_i existe dans la table T. S'il existe, le mot de passe est w_j

Attaques sur les mots de passe

Deviner le mot de passe

- Online: Pour un utilisateur connu U, essayer un ou plusieurs mots de passe séquentiellement (U, P_i). Le serveur indique si le mot de passe est correct ou incorrect
  - Défenses: permettre un nombre limité d'essais, CAPTCHA, Ajouter un délai après chaque essai mauvais
- Offline: Comme online, mais plus difficile (impossible ?) de limiter le nombre d'essais
  - Défenses :
  - Fonctions hash spécialisée: Argon, bcrypt, scrypt
  - hash itératif (password stretching) – $H^d(P_i)$. Haché d fois le mot de passe avant de le stocker. d=1000 limite la vitesse de l'attaque par une facteur de 1000.
  - Salt: ajouter une valeur de haute entropie s_i (p.ex. 128 bits), et stocker (u_i, s_i, $H(p_i+s_i)$)

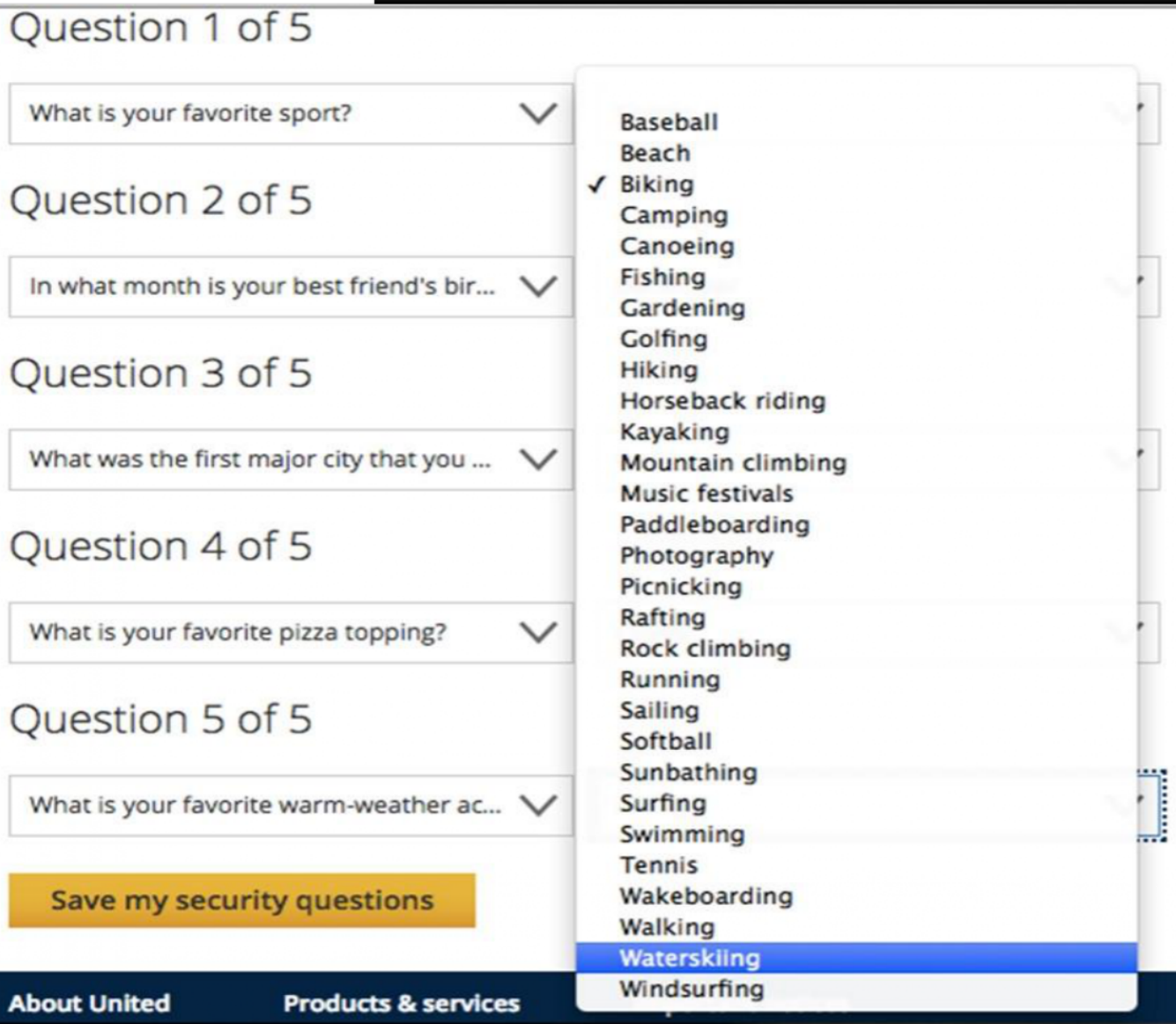
Mot de passe - Récupération

- MP temporaires et liens de récupération
  - Le serveur envoi par courriel un mot de passe temporaire (expiration après quelques heures ou après la première utilisation)
  - Communication par courriel n'est pas chiffrée !

- Question secrètes
  - Lors de l'enregistrement, l'utilisateur répond des questions prédéfinies.
  - Basse entropie pour les questions et souvent pour les réponses !

POLYTECHNIQUE MONTRÉAL
UNIVERSITÉ D'INGÉNIERIE

Mot de passe - Récupération



Gestionnaires de mots de passe

- Gestionnaires de mots de passe
  - Logiciel pour stocker des mots de passe (p.ex. 1password, LastPass, pass, Dashlane, KeePass)
  - Un mot de passe maître pour protéger plusieurs mots de passe
    - AKA « Single Sign-on » (SSO)
  - Avantages
    - Sécurité
      - mot de passe généré automatiquement avec plus d'entropie
    - Convivialité
      - auto-remplissage des champs de mot de passe (« auto-fill »)
      - génération automatique de mot de passe
  - Désavantages
    - Difficulté de synchronisation entre plusieurs PC,
    - Comment choisir un « bon » de mot de passe maître?
    - Point de défaillance unique.
  - « Mettez tous vos œufs dans le même panier, et protégez bien ce panier ! » -- Andrew Carnegie, 1885

Mots de passe – Contremesures

- Algorithme unidirectionnel
  - Introduire une variation aléatoire pour permettre plus d'une variation possible (« salt » en Unix)
  - Utilisation de fonction de hachage cryptographique sécuritaire
- Choix du mot de passe
  - Utiliser plus que 26 caractères: majuscule, minuscules, chiffres et symboles spéciaux
  - Utiliser un mot de passe suffisamment long (« phrase de passe »)
  - Éviter des mots de passe qui sont des mots du dictionnaire(s)
- Politique de gestion de mot de passe
  - Expiration des mots de passe
  - Mots de passe à usage unique : Un mot de passe = Un système
  - Contrôle des mécanismes de mise à zéro (« password reset »)
  - etc.

MOTS DE PASSE = TALON D'ACHILES !!!

Authentification à deux facteurs (2FA)

- Idée
  - Combiner au moins deux facteurs d'authentification
  - En anglais : Two Factor Authentication (2FA) ou multi-factor
  - Chaque facteur a besoin d'une attaque différente
- Méthode « simple »
  - MP + {biométrie OU jeton} + ….
  - Tous les facteurs vérifiés localement par serveur d'authentification
- Méthode « threshold »
  - M de N facteurs doivent être corrects
- Méthode « OTP »
  - MP + Mot de passe à usage unique (One-Time Password)
  - Deux méthodes possibles
    - Méthode locale
    - Méthode à distance (remote)

OTP - Méthode locale

- Dispositif
  - Porte clé avec écran (p.ex. Secure ID)
  - Calculatrice avec écran et clavier (pour entrer NIP)
  - Plateforme mobile avec application sécurisée
  - Chaque dispositif a un ID unique (un par compte)

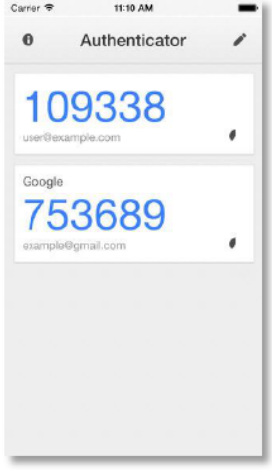
- Méthode
  1. Enregistrement du device

     Secret *S* généré à partir du device ID et une clé maître, e.g. $S = h(K, ID)$
  2. OTP généré localement par le dispositif

     $OTP = h(S, timestamp)$
  3. OTP envoyé par usager via Internet
  4. Serveur vérifie

     Identifie bon ID à partir de nom d'usager

     Calcule S et $h(S, timestamp)$ et vérifie égal à *OTP* envoyé



OTP – méthode « remote »

- Dispositif
  - Téléphone cellulaire
- Méthode
  1. Usager se connecte en indiquant usager et MP
  2. Serveur calcule OTP aléatoire
  3. Serveur obtient no. de téléphone d'usage sur BD
  4. Serveur envoie OTP au téléphone par un autre canal (e.g. SMS), aussi appelé « side channel »
  5. Usager entre OTP et envoie via Internet
- Avantages
  - Force Ève à intercepter deux canaux indépendants
- Désavantage
  - Force l'usager à être sur réseau cellulaire ou avoir un accès à un deuxième canal

Signaux vs. Facteurs d'authentification

- Des signaux d'authentification peuvent être envoyés sans participation de l'utilisateur p.ex:
  - Adresse IP
  - Cookies
  - Géolocalisation
  - Caractéristiques du matériel ou logiciel

- Les signaux peuvent augmenter l'assurance d'une authentification, mais ne peuvent pas être utilisés comme facteur indépendant

Authentification dans les réseaux

- Problématiques additionnelles
  - Interception de la session d'authentification
  - Supplantation du système
  - Replay attacks
  - Session hi-jacking
  - Chess-master attack
    - L'attaquant est au milieu de la communication entre le client et le serveur
    - L'attaquant rejoue la trafic comme une partie d'échecs contre deux adversaires différents

Système de « challenge-response »

- La possession d'une information I authentifie l'utilisateur au système
- Au lieu de dévoiler I,
  1. Le système émet un « challenge »
  2. L'utilisateur répond au « challenge » avec une réponse, que seul quelqu'un connaissant l'information I peut calculer
  3. Le système vérifie que la réponse est bonne
- Avantages
  - Protège contre l'interception
- Désavantages
  - Le système doit connaître I
  - Vulnérable à l'attaque de supplantation
  - Vulnérable à l'attaque de « replay »

Preuves à connaissance nulle

- « Zero-Knowledge Proofs », en anglais

- Protocoles permettant à un démonstrateur P de prouver à un vérificateur V qu'il connaît quelque chose ou est capable de réaliser une tâche, sans que V n'apprenne rien d'autre que ce fait

- Sécurité basée sur des problèmes calculatoire difficiles :
  - Coloriage de graphe (NP-complet)
  - Isomorphisme de graphe (NP)
  - Calcul de résidu quadratique modulo $N = p.q$ (NP)

Preuves à connaissance nulle

- Exemple simple de « Zero-Knowledge Proofs »
  - Une personne A non voyante possèdent deux billes de couleurs différentes
  - A rencontre une autre personne B
  - A utilise le protocole suivant pour savoir si B est un voyant ou un non voyant
- Étape 1 : A présente l'une des deux billes à B et lui demande de regarder la couleur de la bille
- Étape 2 : A présente ensuite l'une des deux billes à B et lui demande si c'est la même bille que la première fois
- A répète N fois l'étape 2
- Conclusion
  - B a une chance sur 2^N de réussir le protocole
  - Si N est grand, la probabilité est faible que B soit non voyant
  - Le protocole est à connaissance nulle car A n'apprend rien d'autre que le fait « B est voyant »

Preuves à connaissance nulle

- Applications en authentification
  - P détient une information I qui l'authentifie auprès du système
  - V émet un « challenge » aléatoire, que seul quelqu'un connaissant I peut résoudre
  - V ne connaît pas I
- Avantages
  - Résout le problème de supplantation
- Désavantages
  - Vulnérable au session hijacking et attaque « chessmaster »
  - Requiert une capacité de calcul chez l'utilisateur