Vers l'authentification invisible et permanente

9 décembre 2022

claude@lemarson.com
https://www.lemarson.com

Sommaire

Vers l'authentification biométrique continue

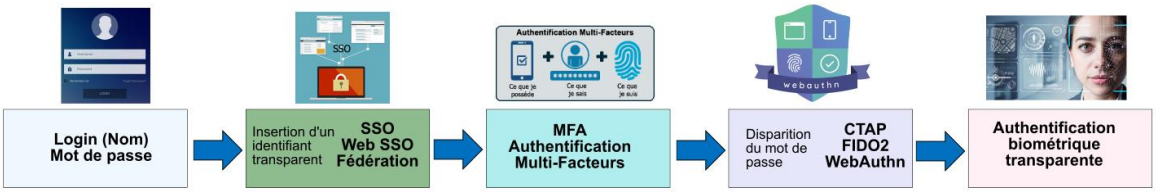
Le marché de la détection biométrique comportementale passe de 1,1 milliard $ en 2020 à 11,2 milliards $ en 2031, avec un CAGR de 23,6 % par an de 2021 à 2031 (Future Markets).

Mot de passe et authentification : inefficacité

- Les utilisateurs font vraiment n'importe quoi (statistiques DataProt).
- 53% font confiance à leur mémoire pour gérer leurs mots de passe (Ponemon Institute).
- 26 % les inscrivent dans un tableur et autant en postits sur l'écran (Ponemon).
- 51% se servent des mêmes mots de passe pour leurs applications professionnelles et personnelles (First Contact).
- 57% des usagers qui ont déjà été attaqués continuent de se server des mêmes "credentials" (First Contact) : "on ne change pas une équipe qui perd"…
- 71% des comptes sont protégés par des mots de passe utilisés sur plusieurs sites (Lawless Research, TeleSign).
- 29% ont plus de comptes protégés dont ils ont perdu la trace (Digital Guardian).
- 90% craignent que leurs comptes soient hackés (Guardian).
- 33% des victimes de compromission de comptes par les mots de passe, ont cessé toute activité avec les services fautifs (Lawless Research, TeleSign).
- Les usagers n'ont pas suffisamment compris qu'un mot de passe et un identifiant c'est un "morceau" de l'entreprise et qu'il faut en prendre soin…
- Les mots de passe forts, les capchas, ne servent à rien…

- Il faut arrêter, trouver "quelque chose" de plus efficace, de non intrusif et permanent.
- Tous les process d'identification, d'authentification doivent être transparents pour l'usager : si on le charge trop, il continuera de faire n'importe quoi.

Les cinq phases de l'authentification

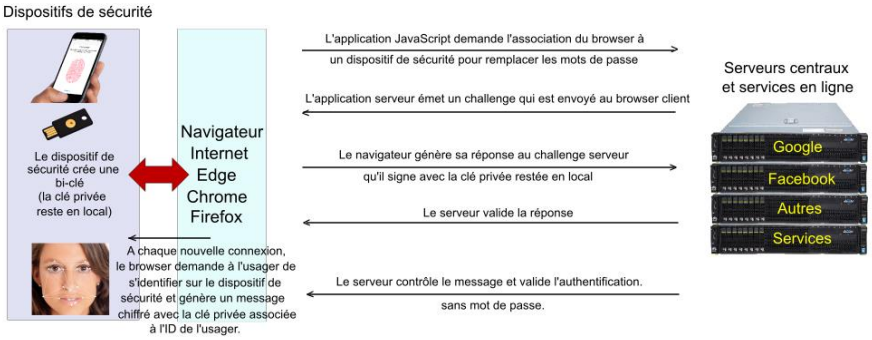


- L'authentification peut être fixe ou dynamique
- Authentification fixe : en début de session
- Authentification dynamique : contrôle permanent sur un ou plusieurs critères

Pourquoi l'authentification basée sur les comportements biométriques

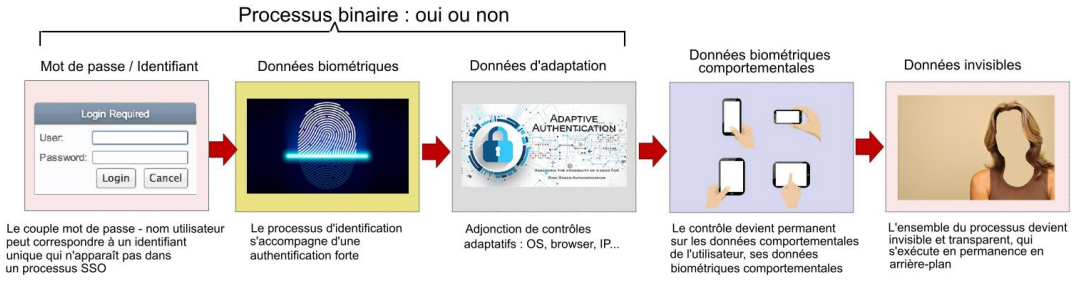
- Aucune technique d'authentification n'est sûre à 100 %, il faut impérativement trouver autre chose, un autre formalisme.
- Un mot de passe, c'est un "morceau" de l'entreprise que l'on confie à un usager : il doit en avoir conscience.
- SSO et WebSSO : il y a toujours un mot de passe, mais il n'y en a qu'un.
- Les protections sont souvent dérisoires (John The Ripper…).
- La plupart des mots de passe sont faibles et réutilisés.
- 80 % des fuites de données importantes sont dues aux mots de passe faibles et compromis (Verizon, 2019).
- L'authentification forte et continue se justifie :
  - Le coût associé à la perte de données confidentielles, peut aller jusqu'à 30 % de celui des centres d'appels.
  - Un prestataire peut être jugé responsable des conséquences d'une attaque : pertes financières et dégradation de l'image.
  - L'authentification forte et fondée sur les comportements biométriques est largement fondée sur les technologies les plus innovantes, de sorte qu'avec le temps elles seront de moins en moins coûteuses à mettre en place et de plus en plus efficaces.

Suppression des mots de passe FIDO2



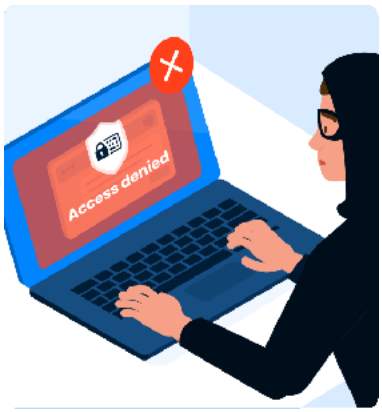
- La déclaration initiale permet à l'usager d'indiquer sa volonté d'utiliser un couple clé/biométrie. Si c'est la première fois qu'il se connecte, l'application serveur lui propose un challenge, un message dans lequel vont se trouver l'IP du demandeur, mais aussi une valeur aléatoire sur 32 octets, qui servira au client pour construire sa réponse.
- Pour répondre au challenge serveur, le dispositif de sécurité du client fabrique une bi-clé, constituée d'une clé publique, qu'il va inclure dans sa réponse et d'une clé privée, qu'il stocke localement et n'est connue que de lui. C'est avec cette clé privée qu'il va signer sa réponse au challenge, qui contiendra le paramètre biométrique choisi.
- Le service va récupérer la clé publique qu'il conserve pour les connexions futures et contrôle que « celui qui répond » est bien celui qu'il prétend être, grâce au déchiffrement qu'il effectue avec la clé publique. Il s'assure que la valeur aléatoire se trouve bien dans la réponse au challenge.
- Ce mécanisme est difficile à circonvenir grâce à la conjonction entre le challenge et sa séquence aléatoire, le jeu de clés générées par le dispositif physique de sécurité et le profil biométrique. Si un attaquant veut pénétrer une session, il lui faudra posséder à la fois la clé privée générée et l'élément biométrique. Ce qui est très improbable. Si quelqu'un s'empare du dispositif biométrique, il ne disposera pas de la clé privée, qui aura été générée à la demande d'enregistrement.
- A partir de là, le processus sera toujours le même. Il suffira au client de faire contrôler son empreinte digitale, s'il a choisi ce dispositif, le browser émettant un message d'authentification signé avec sa clé privée et comportant la fameuse chaîne aléatoire de 32 bytes, que le serveur vérifiera en s'assurant que les demandes de connexion sont signées par celui qui a le droit de le faire, sans avoir besoin pour cela d'un échange de mots de passe.

Cheminement vers l'authentification invisible



L'authentification sera invisible, fondée sur la biométrie comportementale

Comportement biométrique : pour quoi faire ?



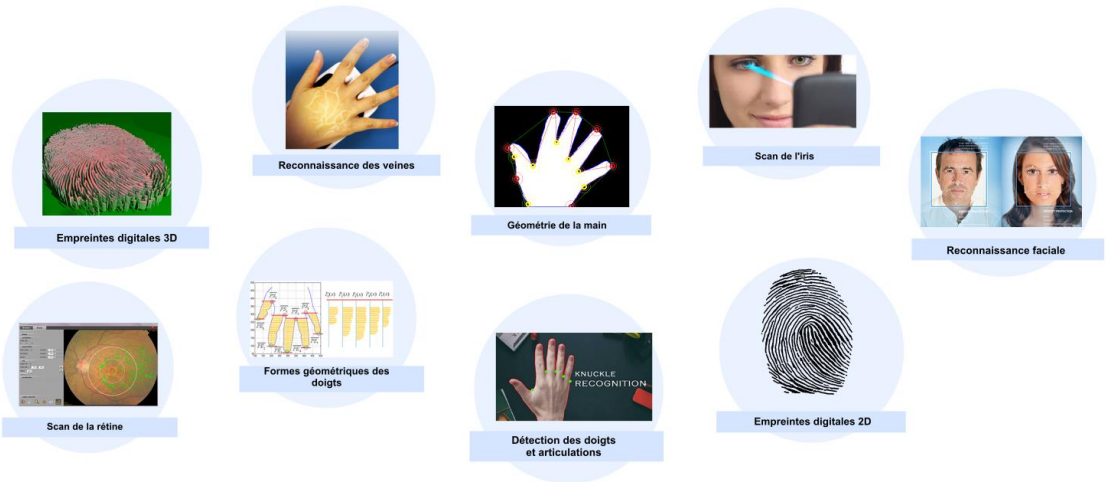
Entre le login initial et l'activité courante, il faut s'assurer que l'utilisateur déclaré n'a pas changé
Le système de contrôle continu vient en complément d'un mécanisme primaire : mot de passe, login…

Ce qu'est le comportement biométrique

- Notre comportement biométrique est plus significatif qu'on ne le croit.
- Il nous caractérise pendant de longues années.
- Il suffit de choisir les bons critères.
- Il concerne :
  - Les mouvements que nous pratiquons
  - Nos attitudes
  - Certaines postures
  - La brusquerie ou souplesse des transitions
  - La vitesse d'exécution
  - La réaction aux événements
- S'applique à tout ce qui est dynamique dans nos comportements

Les critères biométriques possibles

- Les différentes manières d'identifier une entité avec des critères biométriques

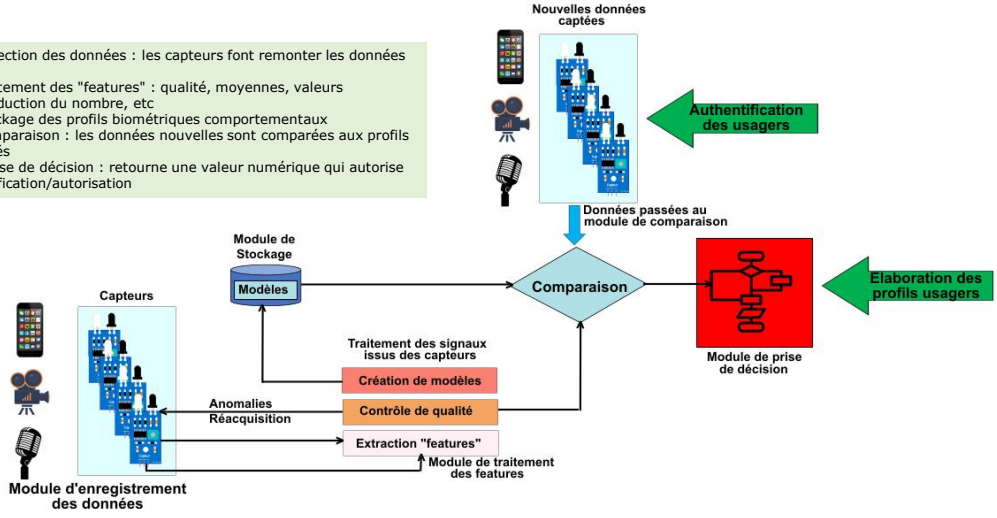


Les comportements possibles

- Discerner les caractéristiques biométriques qui peuvent changer instantanément en fonction d'un événement

Le mécanisme du contrôle

- Module de collection des données : les capteurs font remonter les données brutes
- Module de traitement des "features" : qualité, moyennes, valeurs aberrantes, réduction du nombre, etc
- Module de stockage des profils biométriques comportementaux
- Module de comparaison : les données nouvelles sont comparées aux profils déjà enregistrés
- Modules de prise de décision : retourne une valeur numérique qui autorise ou non l'identification/autorisation



Avantages et inconvénients

Avantages

- Le process ne perturbe pas l'activité des utilisateurs, qui normalement ne s'en rendent pas compte.
- Impossibilité de "stocker" des comportements : ils ne peuvent pas être réutilisés
- Peut se fonder sur des équipements classiques, sans produit spécifique à ajouter, sauf cas avancés fondés sur l'IA et capteurs spéciaux (cerveau…).
- Quand il est appliqué à un domaine restreint, sans rechercher l'universalité, les comportements biométriques sont plus simples à modéliser, plus homogènes et plus aptes à faire ressortir les "anomalies".
- Les comportements biométriques sont très complexes à copier : assemblage de plusieurs "patterns" de comportements.
- Grande fiabilité des résultats.
- Relativement bien accepté, mais avec de grandes disparités selon les pays.

Inconvénients

- L'authentification continue n'est pas un instrument primaire, il doit être associé à un autre élément.
- Le coût d'intégration de la technologie est très élevé, même s'il ne faut pas acquérir d'équipements supplémentaires.
- La mise au point du profil et de ses critères significatifs est complexe.
- Les API sont propriétaires et très peu nombreuses : il faudra faire beaucoup d'efforts pour la faire progresser…
- Le volume de données à acquérir est important.
- Il faut procéder à de constants ajustements dans le construction des profils.
- Enormes problèmes éthiques et de respect des règlementations.

Les solutions

BioCatch
Vitesse de frappe, habitudes de balayage, clics de souris.
HSBC, BARCLAYS, American Express, citi VENTURES, NatWest

typingdna
Dynamique de frappes clavier.
Microsoft Azure, ForgeRock, Optimal IdM, BBVA, Proctoru, Capgemini.

pulse
Combinaison de caractéristiques biométriques statiques avec des comportements dynamiques.

Plurilock
Dynamique de frappes clavier, dynamique de pointage souris.
Agences fédérales américaines.

ZIGHRA
Manières de tenir un téléphone, balayage à l'écran.
Fond d'innovation du gouvernement canadien.

VoiSentry
Identification d'un locuteur et système de vérification.
ForgeRock, University of York, MyForce.

ThreatMark
Evénements de souris, dynamique de frappes, comportement de navigation Web, interactions avec les éléments du site Web.
SLOVENSKÁ SPORITEL (Banque), SBERBANK

cynet
Analyse des comportements biométriques en continu.
Darktrace, Microsoft Azure, Vectra Networks.

BehavioSec
API spécialisée dans la récupération des comportements biométriques.
IDG, Gartner, Goode Intelligence.

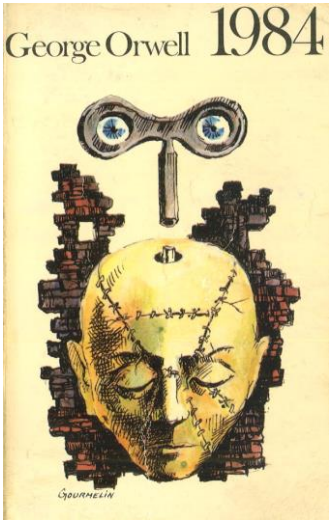
UNIFYID
Techniques d'analyse biométriques sans que les usagers en aient conscience.
Banques américaines.

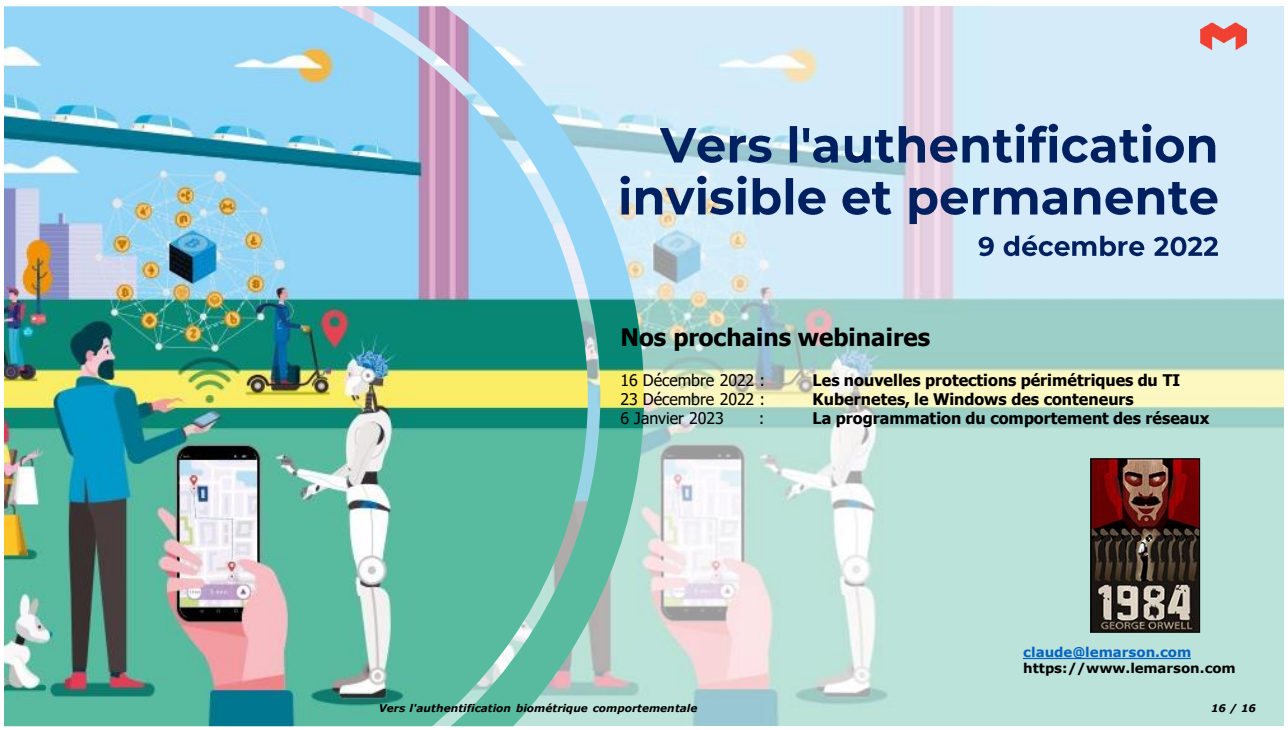
simprints
every person counts
Scanner d'empreintes digitales sans fil.
BRAC, Cohesu.

Acceptto
L'un des leaders de l'identification par analyse des comportements biométriques.
Vue unifiée Web, mobile, centre d'appel, nombreux clients dans les Fortune 500.

Jusqu'où peut-on aller : faux positifs…
et surveillance (George Orwell : 1984)

- Les prochaines années seront décisives qui vont changer profondément les mécanismes d'authentification
- Premiers temps : double authentification statique au départ (puce électronique dans un futur proche), puis dynamique et continue après
- Le risque est de générer des faux positifs : croire qu'un événement n'est pas en phase avec un profil enregistré et agir en conséquence
  - Avec un taux d'échecs de 20 %, les faux positifs seront nombreux… qui perturberont les usagers, interrompus constamment dans leurs activités
- Autre risque majeur : la dérive vers une surveillance Orwellienne : plus rien n'empêchera l'entreprise d'aller plus loin que l'authentification, pour catégoriser les individus en fonction de leur comportement.
- On peut penser que le pouvoir politique ne pourra pas l'empêcher…





Vers l'authentification invisible et permanente

9 décembre 2022

Nos prochains webinaires

16 Décembre 2022 : **Les nouvelles protections périmétriques du TI**
23 Décembre 2022 : **Kubernetes, le Windows des conteneurs**
6 Janvier 2023 : **La programmation du comportement des réseaux**

claude@lemarson.com
https://www.lemarson.com