AWARE

BOOTH
N°C36

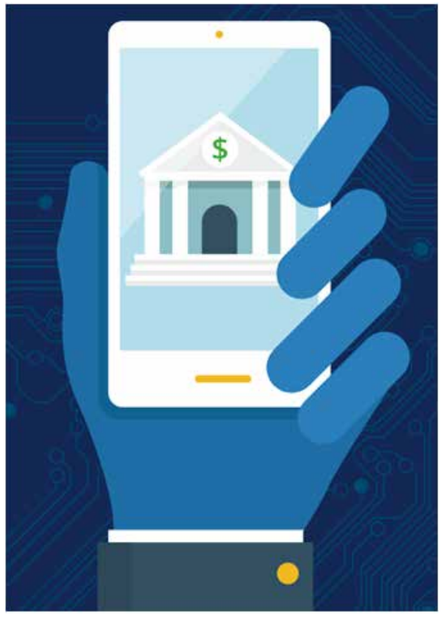
La convergence de la technologie mobile et la Biométrie Multimodale : une puissante identité paradigme pour le nouveau monde numérique

David Benini, Vice-Président Marketing produit, Aware, Inc.

Dans notre monde moderne, un nombre important de nos actions quotidiennes exigent une authentification forte pour protéger les actifs ou pour autonomiser les actions et les transactions. Les vulnérabilités dans ce nouveau monde créent un besoin clair et présent pour renforcer en permanence la sécurité du processus d'authentification sans ajouter des inconvénients pour l'utilisateur. Heureusement que l'émergence d'authentification multifactorielle (AMF) et l'authentification biométriques mobiles crée de nouvelles pistes pour relever ce défi en fournissant un remplacement plus robuste et pratique pour les mots de passe. L'authentification multifactorielle (AMF) rende tâche difficile aux fraudeurs qui souhaitent vaincre les mécanismes de sécurité sans ajouter des inconvénients à l'utilisateur. Tandis que nos dispositifs mobiles offrent une solution convaincante de sécurité ; lorsqu'ils sont combinés avec des mots de passe, ils offrent une authentification à deux facteurs :

1. **Possession**: quelque chose que vous avez ; le smartphone lui-même.
2. **Connaissance:** quelque chose que vous savez ; un mot de passe.

LES MOTS DE PASSE : UN DEMI-SIÈCLE DE TECHNOLOGIE ANCIENNE



Les mots de passe ont été conçus pour un monde numérique beaucoup plus simple, et ils se révèlent aujourd'hui inadéquats. D'abord les mots de passe sont vulnérables à deviner, à « l'hameçonnage », l'interception, aux attaques de force brute, et violations de données à grande échelle. Deuxièmement, les utilisateurs ont un nombre croissant de comptes Web alors que la meilleure pratique est d'avoir des mots de passe différents pour chacun d'entre eux en réalité ils utilisent souvent le même mot de passe, ou ils comptent sur des gestionnaires de mot de passe qui ont également des vulnérabilités. Enfin, des méthodes plus récentes pour améliorer les mots de passe, telles que l'utilisation de questions de sécurité et de mots de passe à usage unique sont également insuffisantes. Une question de sécurité peut être devinée à travers la recherche sur les médias sociaux et les mots de passe à usage unique peuvent être interceptés.

Compte tenu de l'évolution radicale de nos réseaux et dispositifs informatiques qui a eu lieu depuis que les mots de passe ont été inventés, il est évident que les mots de passe sont terriblement précaires et peu pratiques. Ceci est essentiel dans le contexte de l'administration en ligne (eGouvernement), où un nombre croissant de services gouvernementaux seront accessibles en ligne. La biométrie est une alternative intéressante aux mots de passe car ils sont de nature pratique et unique. Ils sont faciles à utiliser mais difficiles à voler et à usurper. Mais chaque modalité biométrique a des caractéristiques uniques qui apportent des avantages et inconvénients en termes de sécurité et de commodité.

LA BIOMETRIE MULTIMODALE

La biométrie multimodale a toujours été considérée comme un moyen d'améliorer la performance en termes de *fausse correspondance* et *fausse non-correspondance* ; car l'utilisation de plus de données biométriques conduit invariablement à de meilleures performances. Cependant plusieurs modes peuvent être utilisés pour améliorer

leur résistance à la fraude. En utilisant plusieurs modalités biométriques, les avantages de chaque une peuvent être exploitées, tout en neutralisant leurs inconvénients respectifs. Cette combinaison de multiples modalités sera crucial en même temps que les méthodes d'usurpation d'identité deviennent plus sophistiqués. Pour mieux illustrer ce point, considérer quelques-unes des méthodes multimodales :

- La biométrie vocale améliorée avec une reconnaissance faciale : Une analyse à temps réel de la façon dont la bouche bouge lorsque l'utilisateur 'transmet' un mot de passe aléatoire permet de s'assurer que la voix et le scan de la reconnaissance faciale sont compatibles et que l'échantillon n'est pas un enregistrement audio ou vidéo de la victime ciblée.

- La dynamique de frappe améliorée avec reconnaissance faciale. Une image faciale peut être capturée pendant que l'utilisateur est en train de taper son nom d'utilisateur. Cela ajoute la reconnaissance faciale à l'analyse sans augmenter le temps de la capture.

Ces méthodes d'authentification multimodale améliorent non seulement la performance biométrique mais rendent également plus difficile pour les fraudeurs d'usurper les analyses biométriques. Ils le font sans impacter négativement l'expérience de l'utilisateur en opérant simultanément. L'authentification biométrique promet de fournir un remplacement moderne et convenable pour les méthodes anciennes de sécurité.

L'IMPLEMENTATION SUR LE PERIPHERIQUE OU LE SERVEUR CENTRAL

Détection de vivacité est essentielle à la mise en œuvre réussie de la biométrie, tout comme la sécurité sous-jacente du stockage biométrique de du moteur de correspondance, qui peuvent être mis en œuvre soit sur l'appareil ou sur un serveur central. Le choix dépend de nombreux facteurs:

- Sécurité des dispositifs : Quelle est la capacité de l'appareil pour sécuriser les données biométriques ?
- Sécurité du serveur : Quelle est la capacité à sécuriser les données biométriques centralisée ?
- Utilité des données basées sur le serveur : est-ce que les données biométriques peuvent être utilisées à autres fins, comme par exemple pour améliorer des algorithmes ou pour vérification contre d'autres données ?
- Évolutivité : Est-il préférable d'ajouter de la complexité à une application ou au backend?
- Capacité de réseau sans fil : Quelle est la taille maximale d'une application pour un téléchargement pratique ? Quel est l'impact sur la vitesse d'authentification ?
- Mémoire de l'appareil et puissance de traitement : Est-ce que de nombreux clients utilisent des appareils moins puissants qui bénéficieront de traitement côté serveur ?
- Normes : A quel point est-il souhaitable d'utiliser une technologie basée sur des normes telle que FIDO ?
- Fonctionnalité multi-appareils : Est-il important que les utilisateurs puissent utiliser plusieurs appareils ?

CONCLUSION

En ce qui concerne la sécurité dans « le monde en ligne », telles que applications « eGouvernement » ou la finance en ligne, adopter une stratégie pour authentification d'utilisateur qui est ancré sur multi-factor par conception. La réalité de la menace en cours nécessitera l'utilisation de plusieurs facteurs pour améliorer la sécurité. Considérer la biométrie multimodale pour leur commodité et accepter que les attentes des utilisateurs nécessitent un accès via une plate-forme mobile. Tourner le défi de la téléphonie mobile en un avantage en misant «mobile » comme un deuxième facteur. Des moteurs d'authentification et des plates-formes tels que ceux proposés par Aware vous permettent de tirer le meilleur parti de votre prise de décision en vous fournissant un cadre personnalisable prêt à être branché à votre application eGouvernement ou à vos plates-formes bancaires.

Aware, Inc. – Biometric Solutions for Mobile Authentication and Identity Proofing www.aware.com