Authentification par mot de passe,bonne ou mauvaise idées ?
Existe-t-il autre chose que le mot de passe ?

Description succincte du sujet :
Questionnement sur le thème de l'authentification en informatique.
Le rapport qu'entretient les utilisateurs et développeurs avec les différentes technologies d'authentification. Et plus spécifiquement l'utilisation de mots de passes dans une application.
L'authentification par mot de passe a longtemps été la norme pour sécuriser l'accès aux comptes en ligne et aux systèmes informatiques. Mais est-elle la meilleur solution ?

Concepts clefs :

- Expérience utilisateur :
Dans l'authentification des applications et des sites web, l'expérience utilisateur est aussi importante que la sécurité. Une interface complexe peut avoir pour effet de repousser l'utilisateur même si la méthode d'authentification est extrêmement sécurisé.
Mots de passe : Même si les utilisateurs sont familiers avec cette méthode, se souvenir et gérer plusieurs mots de passe peut être fastidieux. Les gens ont tendance à utiliser des mots de passe faciles à retenir, ce qui peut compromettre la sécurité. De plus, les systèmes de récupération de mots de passe peuvent être fastidieux à la fois pour l'utilisateur et pour les développeurs.
L'authentification à deux facteurs (2FA) : Ajoute une sécurité supplémentaire en demandant une deuxième étape après le mot de passe. Cette technologie est devenu presque systématique chez des applications de grande envergure. Elle ajoute une surcouche de sécurité mais également des étapes supplémentaires imposé à l'utilisateur.
Biométrie : Offre confort et dynamisme en permettant l'utilisation d'empreintes digitales ou de reconnaissance faciale, éliminant ainsi le besoin de se souvenir des mots de passe. Cependant, certaines personnes s'inquiètent de la confidentialité et de la possibilité que leurs données biométriques soient compromises.

-Impression de sécurité :
L'impression de sécurité est presque plus importante que la sécurité elle même au sain d'une application.
Mots de passe : Le mot de passe n'est plus de nos jours le meilleur moyen de sécurise une application. Cependant l'utilisateur lambda, qui ne s'intéresse pas spécialement au domaine de la sécurité informatique sera toujours rassuré de trouver un système de mot de passe.

- <u>Le SSO</u> (Single Sign-On - Connexion Unique) **:** Le SSO, est un service d'authentification permettant de centralisé la connexion de plusieurs service. L'un des plus connus est celui de Google.
Avantages du SSO :

1. Meilleure expérience pour l'utilisateur : Pas besoin de se rappeler de plusieurs mots de passe, ce qui rend la connexion plus simple et rapide.
2. Facilité de gestion : Ça rend plus facile la gestion des utilisateurs et des accès, car les autorisations peuvent être gérées depuis un seul endroit.
3. Économie de temps et de ressources : Ça réduit le travail du support technique en diminuant les problèmes de connexion et les demandes de réinitialisation de mot de passe, ce qui permet de consacrer plus de temps et de ressources à d'autres parties de l'application.

<u>Technologies mentionnées :</u>

Il est questions de plusieurs techno d'authentification basé sur trois concepts. Tout d'abord, une authentification basé sur qui est la personne avec un id unique par exemple. Ensuite, basé sur ce que sait la personne (ou l'entité) qui se connecte avec un mot de passe ou une question personnelle par exemple. Et enfin, basé sur ce possède physiquement la personne, une clé ou le téléphone avec une notification push par exemple. Il également mentionné l'utilisation de SSO comme celu de google qui permet de centralisé les connexion de plusieurs app.

<u>Applications pratiques :</u>

Magic link (lien magique) : Plutôt que de saisir un mot de passe, certaines applications envoient des liens de connexion uniques par e-mail, ce qui simplifie le processus de connexion pour les utilisateurs sans nécessiter la saisie d'un mot de passe. Utilisé Également pour le système de mot de passe oublié.

Notification Push : Les applications envoient des notifications push aux utilisateurs pour confirmer leur identité ou pour autoriser une connexion sur un nouvel appareil.

WebAuthn : Cette technologie permet une authentification basée sur des clés publiques, offrant une méthode d'authentification forte directement depuis un navigateur web compatible avec des clés matérielles ou intégrées aux appareils mobiles.

<u>Questions que cela soulève chez vous :</u>

Peut t'on réellement confié l'authentification de notre site à un service tierce sans risque de fuites d'info ou encore de blocage de nos service de manière arbitraire ?

Le mot de passe sera t’il encore utilisé dans 15ans ?

Les technos vérifiant qui nous sommes comme la reconnaissance faciale son elles encore fiables avec l’arrivé des intelligence artificielle et des technologies type deep fake ?

Critiques positives/négatives :

Le mot de passe reste l’authentification la plus utilisé et qui est ancré dans les habitudes des utilisateurs elle reste donc essentiels à une app. Cependant elle n’est pas la plus sécurisé ni la plus pratique et cela ne s’améliora pas dans le futur avec toutes les nouvelles technologies qui sont de plus en plus performante.

Conclusion :

L'authentification par mot de passe, bien qu'ancienne et couramment utilisée, présente des inconvénients en matière de sécurité. Les nouvelles méthodes, telles que la 2FA, les technologies biométriques ou le Single Sign-On, offrent des alternatives visant à renforcer la sécurité tout en améliorant l'expérience utilisateur. Cependant, chaque méthode a ses propres défis et risques en termes de sécurité et de confidentialité des données. Il est donc crucial de combiner des pratiques d'authentification robustes avec une sensibilisation continue des utilisateurs pour minimiser les risques liés à l'accès non autorisé et aux violations de données.