LES MOTS DE PASSE SONT-ILS DÉPASSÉS?

AGEFI - 01.07.2022

PLUSIEURS GÉANTS DE L'INTERNET VEULENT ABANDONNER LES MOTS DE PASSE AU PROFIT D'AUTHENTIFICATIONS BIOMÉTRIQUES.

La cybersécurité, qui constitue aujourd'hui une préoccupation majeure du monde économique et politique, repose largement sur les processus d'authentification des personnes autorisées à intervenir sur des systèmes informatiques. Cette authentification, traditionnellement, se fait à l'aide d'un nom d'utilisateur et d'un mot de passe. Mais ce système est désormais accusé de ne pas offrir une sécurité suffisante: les utilisateurs – malgré les mises en garde – se créent des mots de passe beaucoup trop simples, les réutilisent parfois à l'identique sur tous leurs comptes, voire les affichent dans leur bureau ou les transmettent à des tiers.

Plusieurs géants de l'internet annoncent qu'ils veulent abandonner l'usage des mots de passe au profit d'authentifications exclusivement biométriques. Chaque identification se ferait à partir de notre téléphone portable, sur la base de données stockées et chiffrées sur l'appareil et jamais communiquées à l'extérieur.

Nous avons déjà actuellement sur nos téléphones des applications qui nous permettent de nous identifier par reconnaissance digitale ou faciale. Mais ce mode d'authentification est généralement optionnel, activable à choix pour remplacer un mot de passe, ou complémentaire à ce dernier. Vouloir en faire la seule et unique méthode d'authentification pose un certain nombre de problèmes qui vont au-delà des seuls aspects techniques.

Beaucoup d'utilisateurs sont en effet réticents à enregistrer leurs données biométriques, et méfiants quant à l'exploitation qui peut en être faite. Quel serait le degré d'acceptation d'un tel système? Par ailleurs, la sécurité de l'authentification biométrique n'est pas absolue: elle se réfère à des caractéristiques physiques qui sont, dans certaines circonstances, plus directement accessibles qu'un mot de passe enfoui dans notre mémoire. Surtout, et à l'encontre des recommandations actuelles, ces données seraient par hypothèse les mêmes pour toutes nos authentifications; en cas de piratage, les effets seraient beaucoup plus graves.

Parallèlement, les reproches adressés aux systèmes actuels sont de moins en moins justifiés. La création de mots de passe suffisamment sûrs relève certes en première ligne de la responsabilité individuelle, mais cette responsabilité est de plus en plus assistée: lors de la création d'un nouveau compte, divers critères de complexité du mot de passe sont désormais automatiquement exigés et vérifiés. En outre, on voit se répandre les authentifications à deux facteurs, où le mot de passe est complété par un code de contrôle envoyé par SMS.

De fait, la question la plus intéressante qui se pose aujourd'hui – et à laquelle on manque encore de réponses claires et convaincantes – est de savoir quels types d'authentification seront assez résistants face au développement de l'informatique quantique. En attendant d'en savoir davantage, il serait opportun que les géants de l'informatique laissent aux utilisateurs le choix entre plusieurs méthodes d'identification.

Pierre-Gabriel **Bieri**