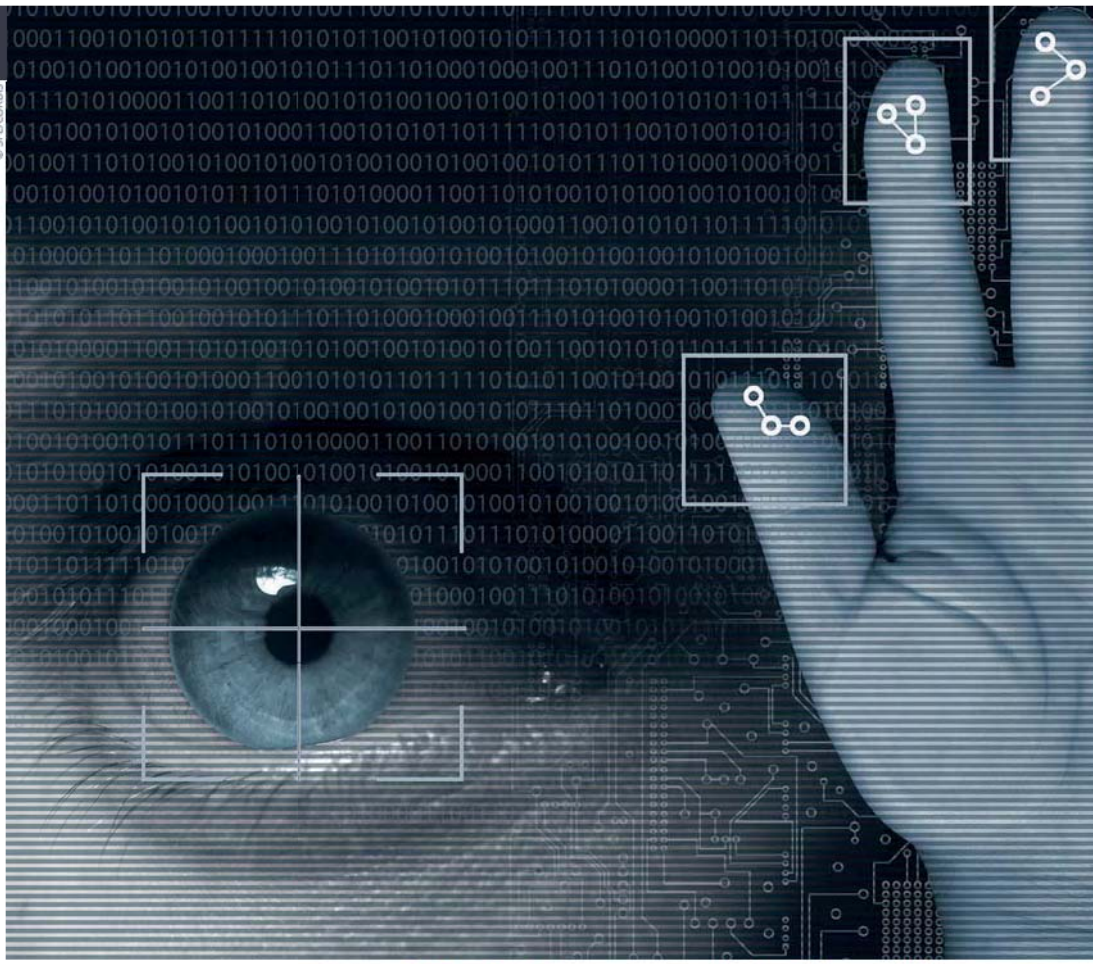

© SPL/CORBIS

NUMÉRIQUE

Biométrie. Après les empreintes digitales, le visage ou l'iris, les chercheurs explorent de nouvelles stratégies d'authentification biométrique, basées sur notre façon de bouger et sur notre manière d'interagir avec nos smartphones.

PAR LÉA GALANOPOULO

Bouger pour s'identifier

L'analyse des gestes pourrait rejoindre le scan d'iris et d'empreintes digitales comme méthode d'authentification.

Pour nous assurer un accès sécurisé aux ordinateurs et aux services en ligne, de plus en plus de parties de notre corps sont susceptibles de passer au scanner afin de nous authentifier. Car nos doigts révèlent bien plus sur nous que nos seules empreintes digitales… Ainsi, depuis 2007, une nouvelle méthode d'authentification biométrique, surnommée avec humour « frappologie », est apparue en France sous la direction de Christophe Rosenberger, professeur des universités à l'Ensicaen, et de son équipe du laboratoire Greyc[1]. L'analyse de la dynamique de frappe au clavier part d'un principe simple : nous possédons tous une façon unique de taper sur notre ordinateur ou notre smartphone. Tendance à enfoncer brutalement les touches ou doigts légers et rapides : la dynamique de frappe trahit facilement notre identité.

« Pour identifier une personne grâce à son style de frappe, nous mesurons trois paramètres : le temps de pression sur chaque touche, le temps de relâchement ainsi que le temps de vol entre deux touches », précise Christophe Rosenberger. Il suffit alors de taper cinq fois un mot de passe personnel pour que le logiciel apprenne la signature de frappe unique à l'utilisateur, à l'aide d'un modèle mathématique. *« Lors de l'authentification, la machine compare le style de frappe du mot de passe tapé au modèle enregistré auparavant pour l'utilisateur »*, ajoute le chercheur.

Simplifier les mots de passe

L'analyse de la dynamique de frappe moderne fonctionne aussi bien avec un clavier classique qu'avec un clavier tactile ou même directement sur une page Web. Elle agit comme une seconde porte de sécurité, couplée avec le mot de passe. Dans seulement 6 % des cas, l'analyse du style de frappe échoue, *« mais en supposant que la personne connaisse déjà le mot de passe »*, souligne le chercheur. Une garantie de sécurité à moindre coût, car cette technique n'impose aucun périphérique supplémentaire, contrairement à d'autres méthodes biométriques. *« Les ordinateurs n'ont pas tous des capteurs d'empreintes digitales, mais ils ont tous un clavier ! »*, relève Christophe Rosenberger.

Dans la pratique, la frappologie intéresse déjà les services de banque en ligne. *« Actuellement, on demande des mots de passe très complexes pour accéder aux comptes, que la plupart des utilisateurs stockent sur leur ordinateur, ce qui est peu sécurisé »*, rappelle le chercheur. En intégrant le style de frappe à l'arsenal de sécurité, les mots de passe pourraient retrouver leur simplicité. Fini, donc, les listes de 15 caractères intégrant ponctuation, chiffres et majuscules !

1. Groupe de recherche en informatique, image, automatique et instrumentation de Caen (CNRS/Unicaen/Ensicaen), équipe « Monétique et biométrie ». 2. Laboratoire d'informatique en image et systèmes d'information (CNRS/UCBL/Univ. Lumière Lyon 2/Insa/Centrale Lyon).

Lire l'intégralité de l'article sur **lejournal.cnrs.fr**

> *« La machine compare le style de frappe du mot de passe tapé au modèle enregistré pour l'utilisateur. »*

Chaque méthode d'authentification possède ses avantages et ses inconvénients. D'où l'intérêt d'en combiner plusieurs. Sur smartphone, le pas est déjà presque franchi avec Google. Le géant américain a lancé le projet Abacus, qui vise à supprimer totalement l'utilisation du mot de passe pour déverrouiller un smartphone en le remplaçant par des méthodes d'authentification biométrique : reconnaissance du visage, de la voix ou même de la façon de respirer ! À ces paramètres s'ajoute l'analyse de la façon dont l'utilisateur interagit avec son portable, développée par Christian Wolf et Natalia Neverova, de l'Insa de Lyon, en collaboration avec Graham Taylor, de l'université de Guelph au Canada. *« Au début, nous n'étions pas sûrs que les données seraient assez efficaces. Mais les résultats montrent finalement que les mouvements sont très corrélés à chaque personne »*, révèle Christian Wolf, maître de conférences au Liris[2], s'appuyant sur les résultats d'une étude préliminaire menée par Google sur 1 500 personnes.

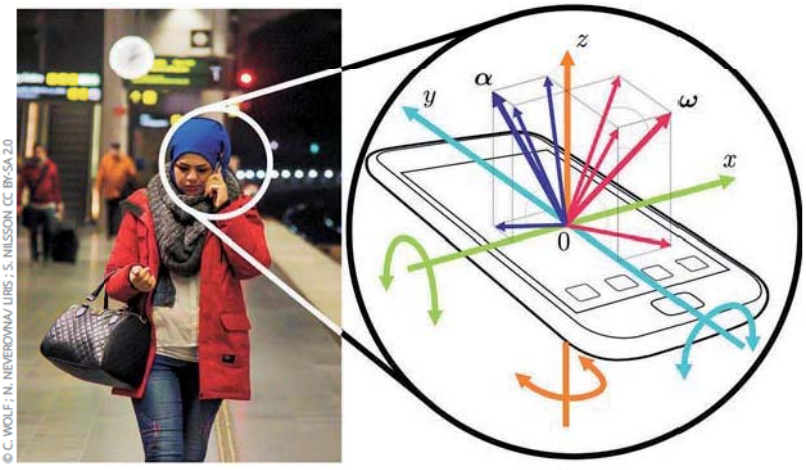
L'analyse de la gestuelle se base sur les capteurs gyroscopiques et l'accéléromètre intégrés dans chaque smartphone. Ils permettent de distinguer finement la rotation et le mouvement linéaire de l'appareil. *« Nous avons conçu un modèle mathématique permettant à la machine d'apprendre à identifier les mouvements et donc l'utilisateur,* explique Christian Wolf. *Basée sur une technique appelée le Deep Learning, le programme est entraîné de manière automatique, à partir d'un grand ensemble de données d'utilisateurs enregistrées par Google. Comme lorsque, dans notre enfance, nous apprenons à distinguer l'image d'un chat, ici la machine apprend à reconnaître une personne via ses mouvements. »* Point positif : ce système ne transmet jamais les données personnelles, qui sont entièrement maîtrisées par l'utilisateur. La machine s'adapte à lui et intègre ainsi en permanence de nouvelles données.

Peut-on frauder la biométrie comportementale ?

En prenant en main son téléphone, l'utilisateur n'aura donc plus à entrer de mot de passe, l'appareil se déverrouillant automatiquement. *« Si, au bout de trente secondes, la machine détecte que ce n'est pas vous grâce aux gestes ou à la reconnaissance faciale par exemple, alors elle se verrouille »*, précise le chercheur. La fiabilité de ce projet paraît presque incroyable… En combinant ces différentes techniques d'identification, l'efficacité est supérieure à celle d'une empreinte digitale ou d'un code PIN.

Seulement, tout comme pour un mot de passe classique, se pose la question de la fraude. Est-il possible d'imiter la manière de frapper de quelqu'un et sa façon de tenir son portable ? Ou tout simplement, est-il possible que ces comportements changent au cours de notre vie ? Pour Christian Wolf comme pour Christophe Rosenberger, ces failles sont envisageables, mais il suffit d'affiner l'algorithme de la machine et de le mettre à jour régulièrement.

La biométrie comportementale interroge également la protection de la vie privée. D'autant plus que l'analyse de la dynamique de frappe pourrait servir au profilage psychologique. *« Nous arrivons à déterminer le genre de l'utilisateur dans près de 80 % des cas »*, souligne Christophe Rosenberger, qui précise que cela fonctionne aussi pour l'âge. Si cela est confirmé, la frappologie pourrait être utilisée pour repérer les pédophiles sur les sites de tchat pour mineurs ou encore pour déceler les faux avis sur les sites de e-commerce… Des techniques *« totalement déployables dès demain »*, ajoute Christophe Rosenberger. En termes d'authentification biométrique, *« la machine semble, dans certains cas, dépasser l'homme »*, conclut Christian Wolf. ▮▮



Un utilisateur peut s'authentifier grâce à ses mouvements mesurés par les capteurs intégrés d'un smartphone.