La Planète du tout mobile

(Article 3/3) - Par Philippe Le Pape, expert sécurité et identité, Vice-Président du développement international et des partenariats au sein de la division Digital Security & Authentication de Safran Identity & Security (ex Morpho).

IDENTITÉ

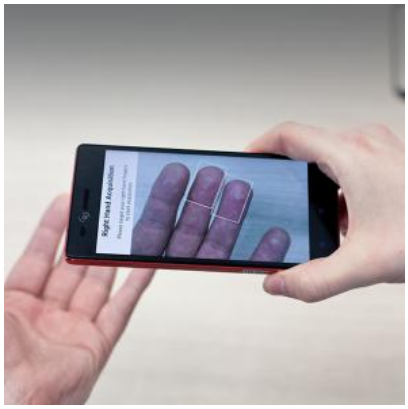
POSTÉ LE 30.06.16

Comme évoqué précédemment, les appareils mobiles régissent notre vie : nos loisirs, nos modes de communication, notre travail et même notre manière de consommer. La technologie mobile – téléphones, tablettes et autres notebooks – a changé notre quotidien plus rapidement que toute autre technologie auparavant. Les conséquences de cette évolution sont nombreuses, notamment sur la manière de communiquer au quotidien, à toute heure et en tout lieu.

La **biométrie** destinée à remplacer les mots de passe des ordinateurs n'est pas un sujet nouveau : les **lecteurs d'empreintes digitales** sont couramment utilisés sur des ordinateurs portables depuis le lancement de Windows XP, en 2001. Toutefois, en raison de l'omniprésence des appareils mobiles, la biométrie a toutes les chances de devenir la méthode d'authentification privilégiée. D'ores et déjà, les lecteurs d'empreintes digitales et les **logiciels de reconnaissance faciale** ont fait leur apparition sur ces appareils.

Et pourtant, c'est bien le format des appareils mobiles lui-même qui a suscité le besoin d'une alternative aux mots de passe traditionnels. La petite taille des écrans, les claviers minuscules difficiles à utiliser compliquent la saisie d'une suite de caractères, d'autant plus que ces appareils sont généralement utilisés en mouvement. La plupart proposent des fonctionnalités, véritables pansements de fortune, pour « retrouver » ses mots de passe, amoindrissant dans la foulée leur niveau de sécurité, en particulier parce qu'un téléphone portable a beaucoup plus de risques d'être perdu ou volé. Mais ce n'est pas tout. Les applications mobiles, y compris celles qui peuvent avoir accès à des mots de passe enregistrés, s'avèrent difficiles à contrôler. Les analystes de la sécurité ont recensé ces applications dangereuses parmi les principaux vecteurs d'attaques. Même les grandes « Applications Stores » ont été victimes d'applications de pillage des données privées au cours de l'année écoulée. En 2014, Symantec a montré que 17 % de l'ensemble des applications Android (près d'un million en tout) étaient en réalité des logiciels malveillants déguisés. Tous ces facteurs exposent l'identité des utilisateurs d'appareils mobiles à des risques supplémentaires. La nouvelle offre biométrique évolue afin de répondre à ces enjeux de sécurité, à l'image de **la plateforme américaine de MorphoTrust, Identix Trusted Identity-as-a-Service (TIaaS)**, qui permet aux développeurs d'intégrer la **vérification de l'identité sur les appareils mobiles** pour un large éventail de services.

Il est intéressant d'observer à ce stade les facteurs économiques qui stimulent la consumérisation du marché de la biométrie. Le marché mondial en 2015 représentait environ 2,5 milliards d'appareils. Il faut également souligner les efforts importants déployés par tous les grands fournisseurs de solutions de paiement qui ont à coeur de faire du smartphone une plateforme de choix en matière de paiement sans contact sécurisé. Une « tempête de perfection » se profile, entraînant la nécessité de mettre la biométrie industrielle au service des appareils mobiles des particuliers. Mobey Forum prévoit avec ces turbulences l'adoption rapide des systèmes biométriques et leur utilisation par plus d'un milliard de personnes d'ici 2017 dans le cadre d'opérations bancaires en ligne.



Quand la R&D s'en mêle

Devenir leader de la biométrie nécessite d'investir de manière considérable dans le domaine de la R&D et de compter sur un savoir-faire développé dans un ensemble de disciplines complémentaires, comme l'acquisition et le traitement d'images, les algorithmes de reconnaissance de formes pour créer des modèles, la cryptographie pour sécuriser les modèles, l'architecture des données pour construire une base de données type, des algorithmes pour la vérification des modèles, et plus encore. Aujourd'hui, les grands protagonistes de la biométrie investissent massivement dans l'optimisation et l'interopératiblité des algorithmes. Selon le rapport de Mobey Forum, les progrès qui en résultent en matière de précision et de rapidité des solutions biométriques sont tels que le centre d'informations du gouvernement fédéral américain sur la biométrie.

> *La plupart des systèmes biométriques ont un niveau de précision élevé (supérieur à 95 %, un grand nombre approchant des 100 %).*
>
> *biometrics.gov*

D'un point de vue pratique, les solutions biométriques ont apporté de l'innovation en matière de déploiement et de simplicité d'utilisation, car la demande en matière de solutions nécessitant un minimum de formation des opérateurs, comme dans le domaine du contrôle aux frontières, a augmenté. La consumérisation de la biométrie, où la simplicité d'utilisation et l'« expérience utilisateur » sont encore plus importantes, continuera de renforcer cette tendance. Prenons l'exemple de l'intégration des **lecteurs d'empreintes digitales** aux smartphones. Si tout le monde a oublié le Motorola Mobility Atrix 4G, premier smartphone à proposer un lecteur biométrique en 2011, chacun se souvient d'Apple qui a ajouté un capteur d'empreinte digitale sur l'iPhone 5s. Comment expliquer cette différence ? Apple a su intégrer pleinement la solution biométrique au système d'exploitation d'iPhone et assure une simplicité d'utilisation qui fait sa réputation. Comme souligné dans le rapport de Mobey Forum, cela a conduit à l'essor immédiat de l'utilisation de la fonction de sécurité de l'iPhone.

Servir et protéger

> *Fervent défenseur de la **biométrie** comme outil d'**authentification**, je suis convaincu que les utilisateurs sauront mettre à profit la simplicité d'utilisation, la précision, la fiabilité et la sécurité offertes par la biométrie dans leurs transactions numériques. Naturellement, la biométrie n'est pas une solution miracle pour lutter contre toutes les formes de fraude. En revanche, elle peut représenter – et représentera – une solution efficace à un grand nombre d'enjeux rencontrés par les prestataires de services et leurs clients.*
>
> *Philippe Le Pape*

Toutefois, la nécessité de proposer des solutions d'**authentification multifacteurs** ne va pas s'estomper. Les systèmes bien conçus pourraient même s'en inspirer. Je suis absolument certain que les appareils que nous utiliserons dans un avenir très proche proposeront à la fois des fonctionnalités d'**authentification biométrique** pour plus de sécurité et

donneront d'autres possibilités à l'utilisateur en cas d'impossibilité d'utiliser ces fonctionnalités (pouvoir passer outre le lecteur d'empreinte digitale, en cas de blessure à la main par exemple).

Les personnes dont la mission consiste à déployer des services ou à créer des solutions pour sécuriser ces services se trouvent face à une difficulté : le manque de compréhension des consommateurs face au niveau de menace pour chaque appareil connecté à Internet. Symantec a enregistré 348 millions d'identités exposées aux risques d'attaques en 2014, dont près de 90 millions dans les secteurs financiers et gouvernementaux. Il reste beaucoup à accomplir en matière de sensibilisation aux enjeux de la cybersécurité. Le Plan d'action national sur la cybersécurité de Barack Obama et la stratégie de cybersécurité de l'Union européenne sont un début, mais le secteur aussi a un rôle à jouer en matière d'éducation et de formation.

Et je défends une autre conviction : le rôle de la biométrie est de garantir que la sécurité et la confidentialité des données des personnes (ou des entreprises) ne soient fragilisées à aucun moment d'une transaction numérique. Le rôle de la biométrie est de servir et de protéger, et non pas d'agir en oppresseur orwellien.