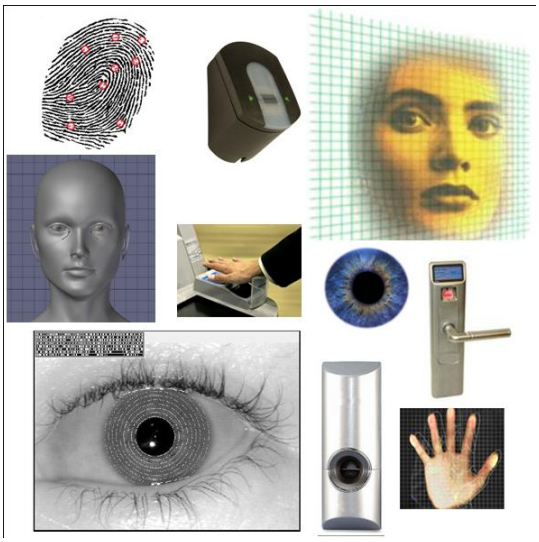
Les risques d’avoir votre mot de passe écrit dans votre corps | Le Net Expert Informatique



Les risques d’avoir votre mot de passe écrit dans votre corps

Reconnaissance faciale, empreinte digitale, reconnaissance vocale. Les marques du secteur du numérique rivalisent d'ingéniosité pour trouver des clés de sécurité en utilisant les données biométriques. Le corps humain est-il devenu « le nouveau mot de passe », l'ultime rempart le plus à même de se protéger contre le piratage de ses données personnelles ?

Jean-Paul Pinte : Comme je le précisais encore il y a deux mois dans différents articles « Rien n'est inattaquable », le corps humain non plus.
Penser que protéger des données au sein du corps humain en faisant de notre corps l'ultime carapace de protection de notre identité et de nos données personnelles n'est pas nouveau.
Elle ne constitue pas non plus à mon sens l'unique solution face aux piratages. Le sujet est certes d'actualité et d'autant plus pertinent que l'on est entré dans l'époque de la traque du renseignement.
En 2002 on évoquait déjà l'avenir de la biométrie dans le Journal du Net. Voici ce que l'on en disait « avec la reconnaissance d'iris et d'empreintes digitales, « scan » de la main et analyse de la voix, autant de technologies qui se banalisent – et qui ne méritent plus leur place dans les films d'anticipation ». Mais patience, nous avons volontairement écarté de notre dossier les technologies qui ne sont pas tout à fait mûres, ainsi que celles qui sont en cours de développement.
Dans quelques années, on devrait ainsi entendre parler de biométrie comportementale, de thermographie et d'ADN. Pour l'instant, ces techniques sont encore dans les laboratoires, mais elles vont progressivement venir renforcer l'arsenal de l'authentification.
Les futurs modes d'identification seront basés et fondés, c'est sûr, en grande partie sur l'analyse de notre corps : rétines, activité cérébrale ou encore la forme de nos veines. Donc des solutions basées sur l'homme. Intel annonçait d'ailleurs, dans ce sens, le lancement de True Key, un système d'identification sécurisé par le biais de la reconnaissance faciale.
Dans un article de l'Atelier du Net on peut également lire que des chercheurs de l'université de Rutgers aux États-Unis, en collaboration avec l'Institut Max Planck et l'université d'Helsinki se sont, quant à eux, penchés sur le dessin ou les formes libres en tant que mot de passe. Ils présenteraient notamment des atouts significatifs en matière de sécurité.

François Dominic Laramée dans un article de « Branchez vous » évoque des chercheurs de l'université de Binghampton, dans l'État de New York, tentant de développer une méthode potentiellement infaillible pour identifier un individu : lire la «signature» de son cerveau.

Aujourd'hui la NSA s'intéresse également à la reconnaissance d'écriture. Après la reconnaissance vocale, la biométrie et son cortège (empreinte digitale, ADN, iris), Facebook cherche à nous reconnaître visage caché. Une technique qui devrait servir encore plus la surveillance.

Paypal inventera une pilule pour que notre corps devienne le meilleur des mots de passe. J'en parlais encore il y a peu de temps.

Toutes ces avancées technologiques, sont pour certaines, fait leurs preuves mais ne sont pas forcément source de fiabilité !

Cette nouvelle technologie, qui utilise les données biométriques, est-elle pour autant (plus) « fiable », moins facile à pirater ?
Jean-Paul Pinte : Il y a encore du travail avant de confirmer définitivement la fiabilité de la technologie biométrique. En effet, comme pour tout domaine d'activité, elle n'échappe pas aux cyber-délinquants qui semblent toujours avoir ce pas d'avance et des parades pour arriver à leurs fins.

Pour la CNIL la biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales.

Les données biométriques sont des données à caractère personnel car elles permettent de trouver ou de vérifier l'identité d'une personne. Ces données ont, pour la plupart, la particularité d'être uniques et stables dans le temps (ADN, empreintes digitales…).

En dix ans, la biométrie a su trouver sa place dans de nombreux domaines, excepté celui de l'authentification. L'empreinte digitale reste encore facilement falsifiable. La technologie par la voix a certes beaucoup évoluée, mais elle n'est utilisée que pour de la dictée ou des commandes vocales. La reconnaissance faciale a trouvé sa place dans la vidéosurveillance, où elle excelle dans l'identification biométrique.

L'iris demeure encore trop mobile pour les capteurs du marché et bute sur des questions de coût. Il bouge beaucoup trop pour réussir une capture fiable, et rares sont les appareils (téléphones ou webcam) équipés d'un capteur suffisamment précis pour réaliser cette empreinte.

S'il s'avère qu'elle n'est pas invulnérable au piratage, quel recours est alors possible ? Que peut-on utiliser d'autre que le corps humain comme moyen de protéger ses données personnelles ?
Quelques projets de recherche ont été menés pour développer des technologies biométriques plus protectrices de la vie privée. Biométrie révocable, anonyme ou cryptage biométrique pourraient être la solution pour concilier confort et vie privée.

Le site Biométrie Online aborde les travaux de thèse professionnelle de Marion Briquet sur le thème « Usages non réguliers de la biométrie : quel équilibre entre confort et vie privée ? ». Cette dernière reprend les avancées des technologies suivantes :

Biométrie « non traçable »
L'objectif de ces technologies de biométrie « untraceable » est de transformer de manière irréversible les données biométriques de la personne afin de ne pas pouvoir remonter jusqu'à elle en les utilisant (« data connectivity »). La notion de « traçabilité » ne se rapporte pas ici à la notion de trace physique laissée par la personne, via ses empreintes digitales par exemple, mais concerne plutôt la façon dont on peut retrouver son identité en utilisant un gabarit de ses données biométriques, laissé dans tel ou tel système.

Cryptage biométrique
Le cryptage biométrique permet de transformer de manière irréversible les données biométriques en données qui ne contiennent aucune information – sur les données biométriques- sources fournies par la personne. Ainsi, aucune donnée biométrique n'est conservée, ni aucun gabarit biométrique.

Biométrie révocable
La biométrie révocable fait également partie des technologies de biométrie non traçable. Il s'agit dans ce cas de créer, à partir de la donnée biométrique, un gabarit « transformé » et non biométrique qui sera le seul conservé. La donnée biométrique n'est pas conservée, comme pour le cryptage biométrique. La comparaison se fait entre les deux gabarits « transformés ». Il est ici aussi possible d'annuler et de renouveler un gabarit.

Biométrie anonyme
Enfin, la biométrie anonyme ou « déidentifiée » (terme préféré par la CNIL) est un dispositif dans lequel les données biométriques ne sont reliées à aucune donnée personnelle permettant d'identifier la personne. Il n'y a pas d'interconnexion avec un autre système où elle pourrait être identifiée. Elle peut être utilisée pour les dispositifs d'authentification seulement, en utilisant par exemple, un tiers de confiance qui authentifierait la donnée biométrique à la demande de la personne ou du fournisseur de service. La seule donnée communiquée serait un numéro de transaction. Cela demanderait de la part du tiers de confiance qu'il mette en place des procédures sécurisées et adéquates d'enrôlement, de conservation, de comparaison…

En dehors de ces recherches approfondies et pour protéger vos données biométriques personnelles le capteur biométrique de la montre Biowatch se met à l'heure du progrès et des objets connectés. C'est ainsi qu'il apparaît plus sûr qu'un autre système d'identification corporel.

Avec la biométrie des veines, les vaisseaux sanguins sont illuminés par une lumière infrarouge qui pénètre de quelques millimètres sous la peau en vue d'analyser précisément les veines. Faire un fake du schéma veineux d'un individu est donc quasi impossible. On imagine vite les avantages de cette technologie car cette identification absolue permet de pallier la perte des mots de passe ou l'égarement de clés voire de cartes d'accès.

Quel type de nouvelle délinquance cela peut-il entraîner ? Assistera-t-on – ou assiste-t-on déjà – par exemple à l'amputation d'un doigt pour récupérer les empreintes digitales ?
Jean-Paul Pinte : Parmi toutes les données biométriques utilisées aujourd'hui l'empreinte digitale présente la caractéristique d'être une « biométrie à trace ». En effet, chaque personne laisse des traces de ses empreintes digitales, plus ou moins exploitables dans beaucoup de circonstance de la vie courante signale la CNIL dans ce dossier.

Par exemple, sur un verre ou une poignée de porte.
A noter que c'est aussi le cas des empreintes génétiques. D'autres biométries ne présentent pas cette spécificité comme le contour de la main ou le réseau veineux en l'état actuel de la technologie nous signale encore la CNIL.

Je vous laisse simplement imaginer le détournement d'une empreinte pour l'identification d'un smartphone et ses dérives possibles aux données contenues dans l'appareil et la projection de cet acte au simple fait d'utiliser cette empreinte dans un paiement ou une identification biométrique. Les gens doivent savoir que l'on collecte des données à leur insu et le risque possible pourrait venir justement de l'utilisation secrète de ces données biométriques, du seul fait que les données sont accessibles au public (photographie des gens, système de balayage des yeux perceptibles à deux mètres, captation des réseaux veineux de la paume de la main et des doigts).

Dans le cas de plusieurs types d'échange avec l'Etat, les personnes n'ont souvent d'autres choix que de se résoudre à communiquer des renseignements personnels qui sont souvent de nature délicate, et ce, parfois en grande quantité. En effet, les données personnelles sont souvent la monnaie d'échange permettant de bénéficier des programmes, des services ou des prestations du gouvernement.

Dans quels domaines cet enjeu est-il le plus prégnant ? On pense par exemple au piratage des données d'entraînement de Chris Froome, le coureur cycliste, ou à la possibilité qui existe par exemple désormais de pirater à distance un pacemaker.
Jean-Paul Pinte : La biométrie est la mesure d'éléments biologiques, comportementaux ou physiologiques uniques et propres à chaque individu. Ses domaines d'action ne manquent donc pas dans notre société mais c'est surtout dans les domaines du Big Data et de l'Open Data, qui touchent entre autres à nos données de santé, qu'il y a de quoi s'inquiéter dès maintenant.

Le risque réside principalement dans la captation des données, leur prise en main et leur exploitation par des personnes mal intentionnées.

La Falco Wheel , dernier vélo fabriqué par une entreprise américaine peut fonctionner comme un outil d'entraînement sportif, mais aussi comme un système de contrôle du rythme cardiaque. Il suffit d'enregistrer, via une application smartphone dédiée, le nombre de pulsations à atteindre ou à ne pas dépasser pendant l'effort. Le dispositif s'occupe du reste. Il en va de même pour le T-Shirt biométrique. Toutes les données sont aujourd'hui facilement traçables voire captables à distance.

Jusqu'ici rien de trop grave dirons-nous ? Allons plus loin et revenons en 2012 avec l'expérience faite uniquement à des fins de preuve de concept. Jack Barnaby a effectué un peu de reverse engineering sur le transmetteur d'un pacemaker. Il a ainsi pu, non seulement, réécrire le firmware de ces appareils mais aussi (et surtout) déclencher des chocs électriques mortels de 830 volts, le tout à une distance d'un peu plus de neuf mètres depuis un simple ordinateur portable.

Le pire résiderait enfin dans le vol de données biométriques effectué sous la menace en vue de diffusion, voire encore de chantage à la donnée comme cela se pratique déjà sur la toile !

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

Cet article vous plaît ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.atlantico.fr/decryptage/votre-corps-comme-mot-passe-rempart-contre-piratage-donnees-qui-est-pas-sans-risque-jean-paul-pinte-2242070.html
Par Atlantico et Jean-Paul Pinte