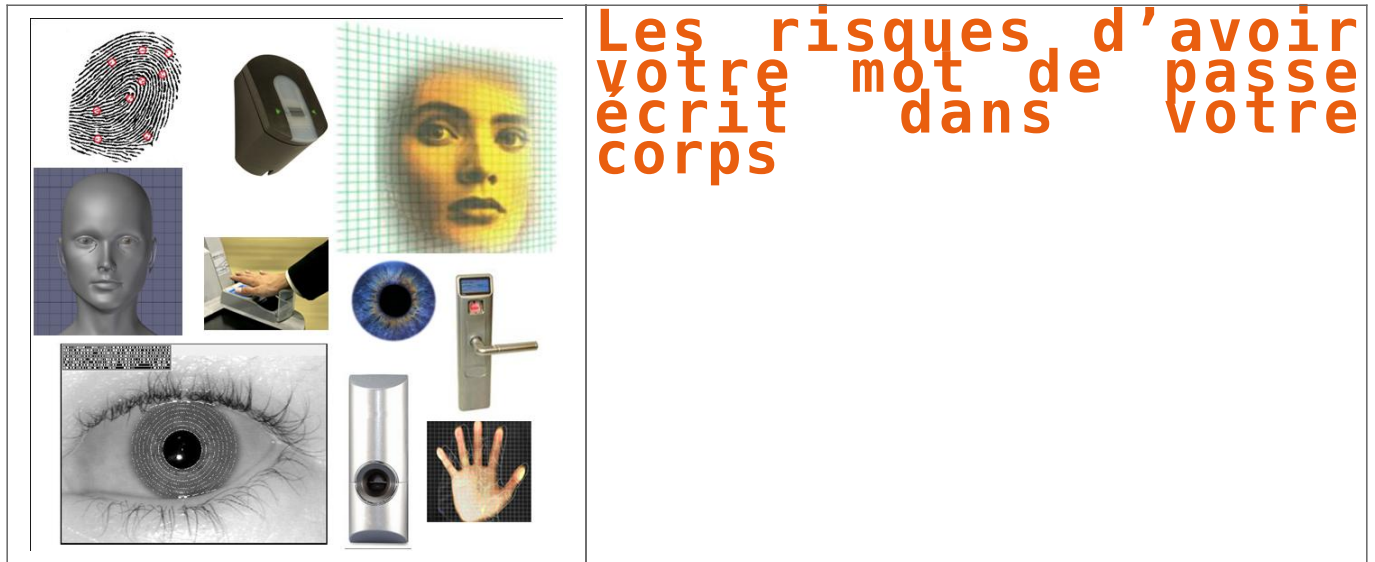


Les risques d'avoir votre mot de passe écrit dans votre corps | Le Net Expert Informatique



Reconnaissance faciale, empreinte digitale, reconnaissance vocale, les images du scanner de rétine risquent d'ingénierie pour trouver des clés de sécurité en utilisant les données biométriques. Le corps humain est-il devenu « la monnaie jet de passe » ? L'Utah reçoit le plus à séduire de se protéger contre le piratage de ses données personnelles ? Jean-Paul Fata : Comme je le précisais encore il y a deux mois dans différents articles « Rien n'est inviolable » . Le corps humain non plus. Même des progrès de données de mise du corps humain en français de notre corps et de nos données personnelles n'est pas nouveau. Elle ne constitue pas un plus à nos l'unique solution face au piratage. Le sujet est certes d'actualité et d'actuel plus porteurs que l'on est entré dans l'ère de la fraude du renseignement. En 2011 un document signé l'Union de la biométrie dans le Journal de Bio. Voici ce que l'on en dit : « sans la reconnaissance d'être un d'empreinte digitale » . « mise de la base et analyse de la voix, autant de technologies qui se banalisent » - et qui se banalisent plus leur place dans les films d'anticipation » . Mais surtout, nous nous volontiers devant de notre dossier les technologies qui ne sont pas tout à fait sûres, aussi que celles qui sont en cours de développement. Mais quelques années, on devrait aussi envisager par la biométrie et d'ADN. Pour l'instant, ces technologies sont encore dans les laboratoires, mais elles sont progressivement pour renforcer l'arsenal de l'authentification. Les films nous d'identification seront bons et sûrs, c'est sûr, en grande partie sur l'analyse de notre corps : rétine, activité cérébrale ou même la forme de nos veines. Pour des solutions basées sur l'Union. L'état monnaie d'échange, dans ce cas, la banalisation de l'Union, ou système d'identification sécurisé par le biais de la reconnaissance faciale. Dans un article de l'Harvard de Net on peut également lire que des chercheurs de l'université de Rutgers au état-Uni, en collaboration avec l'Institut Max Planck et l'université d'Edimbourg se sont, quant à eux, penchés sur la densité ou les formes libres en tant que jet de passe. Ils présenteront notamment des études significatives en matière de sécurité. L'agence fédérale travaille dans un article de « Business week » . « depuis des chercheurs de l'université de Birmingham, dans l'état de New York, tentent de développer une méthode potentiellement efficace pour identifier un individu : lire la signature de son cerveau. Acquiescer la FBI s'intéresse également à la reconnaissance vocale. Après la reconnaissance vocale, la biométrie est un langage empreinte digitale, ADN, etc), Facebook cherche à nous reconnaître chaque année. Une technique qui devrait servir encore plus la surveillance. Apple continue une quête pour que notre corps devienne le meilleur des jets de passe. L'un précise encore il y a peu de temps : Toutes nos données technologiques, ont pour certaines, fait leurs preuves mais ne sont pas forcément source de fiabilité : Cette nouvelle biométrie, qui utilise nos données personnelles, est-elle plus sûre (plus fiable) , mieux facile à gérer ? Jean-Paul Fata : Il y a encore du travail avant de continuer définitivement la fiabilité de la technique biométrique. En effet, comme pour tout données d'activité, elle s'échappe pas nos cyber-délinquants qui semblent toujours avoir ce jet d'absence et des données pour arriver à leurs fins. Pour la FBI, 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...). De nos jours, la biométrie a vu trouver son plus grand domaine d'application, comme c'est le cas de l'authentification. L'empreinte digitale reste encore l'outil le plus fiable. La biométrie par la voix a certes beaucoup évolué, mais elle n'est utilisée que pour de la sécurité ou des commandes vocales. La reconnaissance faciale a trouvé sa place dans la vidéosurveillance, de elle occupe dans l'identification biométrique. L'Union demeure encore trop naïve pour les capteurs du monde et dans les questions de code. Il s'agit beaucoup trop pour réaliser une capture fiable, et même sans les appareils (téléphone ou autres) depuis d'un capteur suffisamment précis pour réaliser cette empreinte. C'est d'ailleurs qu'elle n'est pas soumise au piratage, quel risque 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 sécurisées de la vie privée. Biométrie résolvable, comme du cryptage biométrique pourrait être la solution pour concilier confort et vie privée. Le site Biométrie InfoLab aborde les travaux d'Alexa professional de Marcus Briquet sur le thème « Risques non réglés de la biométrie : quel équilibre entre confort et vie privée ? ». Cette dernière reprend les données des technologies suivantes : Biométrie « non résoluble » L'aspect de ces technologies de biométrie « non résoluble » est de transformer de manière irréversible les données biométriques de la personne afin de ne pas pouvoir remonter jusqu'à elle en les utilisant (ie 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 le fait que d'un point de vue on peut retrouver son identité en utilisant un gabarit de ses données biométriques, laissés 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 résolvable La biométrie résolvable fait également partie des technologies de biométrie non résoluble. 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 La biométrie anonyme ou « dissimulée » trouve également sa place dans la biométrie. Elle est basée sur la notion de données biométriques qui sont reliées à une donnée personnelle permettant d'identifier la personne. Il n'y a pas d'interférence avec un autre système de elle pourrait être identifiée. Elle peut être utilisée pour les dispositifs d'authentification eux-mêmes, en utilisant par exemple, un tiers de confiance qui authenticerait la donnée biométrique à la demande de la personne ou de fournisseur de services. La notion de données biométriques serait un moyen de transaction. Cela dépendrait de la part de tiers de confiance et des protocoles sécurisés ou adaptés d'encodage, de conservation, de cryptage. En matière de ces recherches approfondies et pour protéger nos données biométriques personnelles la notion biométrique de la notion Biométrie 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. Si la biométrie des veines, les véhicules peuvent être illégaux par une dernière surveillance qui pénètre de quelques millimètres sous la peau en vue d'analyser précisément les veines. Faire un film 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 jets de passe ou l'agacement de clés voire de cartes d'accès. Noté que nouvelle allégeance cela peut-il entraîner ? Avez-vous-t-on – un système-tu d'ADN – par exemple à l'application d'un chip pour récupérer les empreintes digitales ? Jean-Paul Fata : Pour 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 circonstances de la vie courante signale la FBI 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 la couleur de la peau ou le réseau veineux en l'état actuel de la technologie nous signale encore la FBI. Je vous laisse imaginer l'impact de la biométrie d'un scanner et ses données personnelles nous données continues 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 sécurisée de ces données biométriques, du seul fait que les données sont accessibles au public (photographie des gens, vidéos de vidéos des gens, données de données de la peau de la main et des doigts). Dans le cas de plusieurs types d'échange avec l'Etat, les personnes s'ont souvent d'autres choses 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 présent ? On passe par exemple au piratage des données d'entraînement de Chris Frantz. Le risque cryptique, ou la possibilité qui existe par exemple d'accéder à des données à distance au paramètre. Jean-Paul Fata : La biométrie est la notion d'éléments biométriques, comportementaux ou physiologiques utilisés et présentés à l'homme. Les données d'activité ou même le mouvement dans un autre système sans c'est un fait dans les données de Big Data et de l'Open Data, qui touchent entre autres à nos données de santé, qu'il y a de quoi s'inquiéter des risques. La risque réside principalement dans la capture des données. Leur prise en main et leur exploitation par des personnes non intentionnées. La Fata Wheel : derrière cela fabriqué par une entreprise américaine peut fonctionner comme un outil d'entraînement sportif, mais aussi comme un système de contrôle de 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 se va de même pour la T-shirt biométrique. Toutes les données sont aujourd'hui facilement traçables voire capitalisées à distance. Insistez bien de trop gros risques non ? Alors plus tard et remonte en 2012 avec l'expérience faite récemment à des fins de groupe de concept. Jack Barmby a effectué un peu de reverse engineering sur le transmetteur d'un paramètre. Il a ainsi pu, non seulement, récupérer le firmware de son appareil 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 fait résident entre dans le vol de données biométriques effectués sous la main en vue de diffusion, voire encore de partage à la donne comme cela se pratique d'ADN sur la table : Experte informatique expérimenté et formateur spécialisé en sécurité informatique, en cybersécurité et en détection à la FBI, Denis JACQUES est le Net Expert tant en matière 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.artefact.fr/descriptiv/votre-corps-comme-est-passe-repert-contre-piratage-donnees-qui-est-que-cas-risque-jean-paul-fata-2202078.html Par Sébastien et Jean-Paul Fata
