Votre crédit bientôt refusé à cause de vos amis Facebook ? | Le Net Expert Informatique

	Votre crédit bientôt refusé à cause de vos amis Facebook ?

Le réseau social a déposé un brevet qui permettrait aux banques de scruter les contacts d'un client afin de déduire sa capacité à rembourser un crédit.

Et si votre assureur savait tout de votre état de santé… Le smartphone tuera-t-il la carte bancaire (et les banques) ?
A quoi joue Facebook ? Un brevet, déposé mardi 4 août, pourrait permettre aux banques d'examiner les relations d'un utilisateur sur le réseau social avant de lui accorder (ou non) un prêt.
Intitulé « Autorisation et authentification basée sur le réseau social de l'individu », le brevet entend proposer une nouvelle méthode d'authentification de l'internaute en fonction de ses amis Facebook, afin de limiter la propagation de spams (messages indésirables) et d'améliorer les résultats du moteur de recherche. Néanmoins, cette technique sera proposée à « des tiers », en particulier des banques. Le texte spécifie :
Lorsqu'un individu demande un prêt, le prêteur examine les scores de crédit des membres du réseau social de cet individu via un nœud autorisé. Si le score de crédit moyen de ces membres atteint le score de crédit minimum, le prêteur continue d'examiner la demande de prêt. Sinon, la demande est rejetée. »
En somme, si vos amis Facebook ont du mal à rembourser leurs prêts, alors la banque pourrait refuser de vous en accorder un. C'est une blague ? Non.

Des start-ups américaines sur la brèche
Généralement, les banques se basent sur l'historique financier pour déterminer la fiabilité d'un client, mais cette procédure est impossible si un tel historique n'existe pas. Du coup, les tentatives se multiplient pour éviter les personnes « à risque » en fonction des informations publiées sur les réseaux sociaux. Plusieurs start-ups s'en sont fait une spécialité.
Lenddo part du principe que si vos amis sont pauvres ou de mauvais payeurs, alors vous devez l'être aussi. L'entreprise américaine parcourt ainsi Facebook pour déterminer si le client potentiel est ami avec une personne ayant déjà remboursé un prêt en retard ou, pire, s'ils interagissent régulièrement.
La société LendUp, spécialisée dans le prêt en ligne, examine elle les comptes Facebook et Twitter des demandeurs, observant notamment le nombre d'amis et les interactions, afin d'accorder ou non le prêt.
De son côté, InVenture se base sur les données recueillies par le smatphone. Une application est proposée aux consommateurs pour gérer ses dépenses quotidiennes, tandis qu'un « score de crédit » est calculé en fonction des frais. Score qui sera fourni aux banques, afin de déterminer la capacité du client à rembourser un prêt.
Et même pas besoin d'appli : l'économiste Daniel Björkegren a montré qu'il suffit de croiser les dépenses des emprunteurs avec l'historique et la durée de leurs appels téléphoniques, pour réduire les défauts de paiement de 42%.

Illustration de l'ogre Facebook (Dimitris Kalogeropoylos/Flickr/CC)

En France, l'étape du « partenariat »
En France aussi, les rapprochements entre banques et réseaux sociaux commencent timidement. Début juillet, la Banque postale s'est associée avec Facebook pour que ses conseillers ouvrent des comptes sur le réseau social afin de rester en contact avec leurs clients. S'agira-t-il aussi de scruter les profils ? La banque ne s'épanche pas là-dessus, vantant la « prolongation de la relation client ».

A la mi-juillet, BNP-Paribas s'est alliée à Facebook, mais aussi Google, Twitter et LinkedIn afin d'améliorer « la pertinence de ses offres en fonction des attentes des clients ». La banque devrait ainsi bientôt proposer d'ouvrir un compte directement depuis Facebook.

La banque marche dans les pas du groupe BPCE (Banque populaire et Caisse d'épargne), allié à Facebook depuis la fin mai, dans une optique de proposer des « offres et produits innovants ». BNP-Paribas et BPCE n'ont en revanche pas précisé s'ils pourront récupérer des données de Facebook sur leurs clients.

CNN souligne néanmoins que les établissement bancaires rechignent encore à utiliser les données personnelles des réseaux sociaux pour évaluer le risque d'un crédit. « Ces données sociales n'indiquent pas nécessairement la fiabilité d'un client à rembourser un prêt à temps », note d'ailleurs John Ulzheimer, expert économique interrogé par la chaîne.

Alors, faut-il se précipiter sur son compte Facebook pour faire le tri parmi ses amis, avant que le nouveau brevet ne soit utilisé ? Pas sûr. Le site spécialisé Presse-citron tempère :

Les entreprises comme Google, Microsoft ou Facebook déposent de nombreux brevets, mais tous ne sont pas utilisés. Il est fort possible que Facebook n'utilise jamais ce brevet ou du moins pas la partie qui risque de vraiment fâcher ses utilisateurs. »

Source : http://tempsreel.nouvelobs.com/tech/20150807.OBS3843/votre-credit-bientot-refuse-a-cause-de-vos-amis-facebook.html#xtor=EPR-1-Actu8h-20150808
Par Boris Manenti

Les e-mails de hauts gradés de l’armée américaine piratés | Le Net Expert Informatique

	Economie – Les e-mails de hauts gradés de l’armée américaine piratés

Le système de messagerie utilisé par 4 000 hauts gradés de l'armée américaine a été compromis fin juillet par des pirates informatiques et fermé par le Pentagone, selon les médias américains. L'enquête privilégie la piste russe.

Comme un air de Guerre froide. Des « officiels » du Pentagone ont affirmé, jeudi 6 août, à la chaîne américaine NBC, que des pirates informatiques russes avaient réussi à s'introduire dans le système de messagerie informatique utilisé par 4 000 militaires et civils travaillant au Comité des chefs d'état-major interarmées.
La découverte de cette opération de cyberespionnage, lancée aux alentours du 27 juillet, a amené les autorités militaires à fermer entièrement le système de messagerie informatique utilisé par ces hauts gradés. Il ne sera remis à disposition du personnel qu'à la fin de l'enquête.

Cyber Guerre froide ?
Cette attaque est d'autant plus dommageable pour le Pentagone que ce n'est pas la première fois que des cyberespions s'engouffrent dans une faille du système de protection informatique des plus hautes sphères de l'État. Le président américain Barack Obama et le Département d'État (ministère américain des Affaires étrangères) ont ainsi déjà été pris pour cible ces quatre derniers mois.
Ces précédentes opérations avaient été attribuées par plusieurs entreprises de sécurité informatique à un même groupe : Cozy Bear. Leurs membres seraient russes, estiment la société Kaspersky qui leur a consacré plusieurs rapports.
Interrogé par le quotidien britannique « The Guardian », Dmitri Alperovitch, le fondateur de la firme de sécurité informatique CrowdStrike, a noté une recrudescence des attaques informatiques russes visant des cibles américaines depuis l'instauration des sanctions économiques imposées depuis plus d'un an à la Russie par les États-Unis et ses alliés.

Pas de vol d'informations classifiées
Mais même si l'attaque contre le Pentagone est bien le fait de pirates russes, rien n'indique qu'ils ont agi sur ordre du Kremlin. Il peut s'agir de hackers « patriotes », souligne le site « Daily Beast », ou d'un groupe indépendant de pirates informatiques recruté par n'importe quel autre pays ou organisé pour espionner à sa place.
Ils ont à chaque fois utilisé la même technique : un e-mail piégé envoyé à des employés du service visé qui installe un virus dès que l'un d'eux clique sur un lien contenu dans le message. Des similitudes dans les messages et des traces laissées par les pirates sur les ordinateurs indiquent qu'ils ont utilisé les mêmes « armes » (comme un même type de virus personnalisé) pour commettre leur forfait.
Lors de l'attaque contre les hauts gradés du Pentagone, aucune information classifiée, qui ne s'échange que sur une messagerie spécifique, n'aurait été dérobée par ces pirates informatiques, ont affirmé ces sources à plusieurs médias américains. Reste que des échanges, comportant peut-être des informations personnelles sur les membres du premier cercle de l'armée américaine, ont été volés.

Source : http://www.france24.com/fr/20150807-emails-militaires-hauts-grades-armee-americaine-piratage-hacking-russie-pentagone
Par Sébastian SEIBT

La SNCB victime d’un piratage | Le Net Expert Informatique

La SNCB victime d’un piratage

Les systèmes de paiement électroniques de la société ferroviaire sont la cible d'une attaque informatique depuis plusieurs heures.

Les systèmes de paiement électroniques de la SNCB sont la cible d'une attaque informatique depuis plusieurs heures. « Il s'agit d'une attaque d'origine externe dont les premiers signes ont été détectés mercredi soir, confirme la porte-parole, Nathalie Pierard. Nous travaillons avec les services de sécurité informatique du Fédéral pour protéger nos serveurs.» Ce sont les systèmes de paiement électroniques qui sont touchés, tant aux guichets qu'aux automates ou sur le mobile.
« Par période, les services sont fortement ralentis, poursuit Nathalie Pierard. À d'autres, ils sont inaccessibles. On a connu une accalmie vers midi puis les ralentissements ont repris en milieu d'après-midi. »

Pas de surfacturation à bord
Suite à ce piratage dont l'origine est toujours indéterminée, la SNCB a décidé de ne pas faire payer la surfacturation de sept euros pour les billets achetés dans le train.

Source : http://www.lesoir.be/956193/article/economie/2015-08-06/sncb-victime-d-un-piratage

Un email constitue une commande ferme | Le Net Expert Informatique

Un email constitue une commande ferme

Voici un arrêt qui pourrait bien, à nous Experts Informatique, nous servir de référence.
Denis JACOPINI

Par un arrêt du 1er juillet 2015, la Cour de cassation considère qu'un courrier électronique envoyé par une société à un expert-comptable lui demandant une réponse étudiée sur trois questions précises, relatives à la fiscalité en Tunisie, constitue une commande ferme de prestation.

Une semaine après sa demande, l'expert-comptable lui avait envoyé sa consultation répondant aux questions posées ainsi que la facture correspondante.
La Cour casse le jugement du tribunal de commerce de Nanterre qui avait considéré qu'il s'agissait d'une simple prise de contact et d'une demande de renseignement général et des conditions financières d'intervention éventuelle.
Elle a estimé que l'email qui appelait à des réponses étudiées aux trois questions posées constituait une commande de consultation, présentée en termes clairs et précis.
Le lien vers la décision de la Cour de Cassation

Source : http://www.legalis.net/spip.php?page=breves-article&id_article=4690

La Cnil met en demeure 13

sites de rencontre | Le Net Expert Informatique

La Cnil met en demeure 13 sites de rencontre

Meetic, Attractive World ou Adopte un mec figurent dans une liste de 13 sites de rencontre mis en demeure par la Cnil pour leur mauvaise gestion des données de leurs membres.

La Cnil veut éviter un scénario à la Ashley Madison en France. Ce site américain de rencontres extra-conjugales a été piraté la semaine dernière. Les données de quelque 37,5 millions de membres, aussi sensibles soient-elles, ont été dérobées. Alors la Commission nationale de l'informatique et des libertés a mené l'enquête auprès de plusieurs sites de rencontre… et annonce la mise en demeure de 13 d'entre eux.
Meetic, Attractive World, Adopte un mec, Easyflirt, Rencontre obèse, Destidyll, Forcegay, Mektoube, Jdream, Feujworld, Marmite love, Gauche rencontre, Celibest. C'est la liste retenue par la Commission, qui leur reproche à tous « de nombreux manquements à la loi informatique et libertés ».

Les voici :
• ne pas recueillir le consentement exprès des personnes pour la collecte de données sensibles, comme celles relatives à la vie et aux pratiques sexuelles, aux origines ethniques, aux convictions et pratiques religieuses ou aux opinions politiques ;
• ne pas supprimer des données de membres ayant pourtant demandé leur désinscription ou ayant cessé d'utiliser leurs comptes depuis une longue durée ;
• mettre en œuvre des fichiers afin d'exclure des personnes de l'accès au service sans avoir procédé à des demandes d'autorisation auprès de la Cnil ;
• ne pas informer correctement les internautes de leurs droits (accès, suppression, rectification) ni des conditions dans lesquelles des cookies sont déposés sur leur ordinateur.
Dépourvue de pouvoir de sanction, la Cnil peut désigner un rapporteur qui décidera, lui, d'une peine –

Crédit : Pic Rider (Fotolia)

Le spectre d'une mauvaise pub
Concrètement, ce sont les sociétés éditrices (8 au total) des sites de rencontre qui sont mises en demeure. Habituellement, une telle procédure n'est pas rendue publique par la Cnil. Une exception que justifie la Commission par la « sensibilité des données en cause » ainsi que « le nombre de personnes concernées ».
Les entreprises visées ont un délai de trois mois pour se conformer à la loi. « La clôture de chacune des procédures fera également l'objet d'une publicité », agite la Cnil, pour les motiver à améliorer leur politique de gestion des données. Dans le cas contraire, elle désignera un rapporteur chargé d'étudier des sanctions pouvant atteindre 300 000 euros selon Les Echos. Mais surtout, une mauvaise publicité leur sera faite.

Source : http://pro.clubic.com/legislation-loi-internet/cnil/actualite-775064-cnil-sites-rencontre.html
Par Thomas Pontiroli

Les objets connectés deviendraient des témoins ? | Le Net Expert Informatique

Les objets connectés deviendraient des témoins ?

Aux Etats-Unis, on commence à produire les données de bracelets connectés pour démentir ou renforcer un témoignage. Ces données pourraient aussi entrer dans nos tribunaux, ce qui n'est pas sans poser question.

A quoi servent les objets connectés « portables », ces bracelets ou ces montres qui permettent de mesurer votre activité physique, vos dépenses en calories et même parfois votre humeur ?
A mieux se connaître, répondent les amateurs. A mener une vie plus saine. Mais une histoire récente, aux Etats-Unis, montre que ces objets peuvent aussi servir lors de votre procès.

Et là, son FitBit a lâché le morceau
Une femme de 43 ans qui avait porté plainte pour viol a été démentie par les données de son FitBit (bracelet connecté mesurant l'activité et le sommeil). L'histoire a été rapportée la semaine dernière par la chaîne d'information locale ABC 27 News.
La femme avait affirmé aux enquêteurs qu'un homme s'était introduit au milieu de la nuit dans sa chambre et l'avait menacée avec un couteau avant de la violer. Mais son gadget a contesté ses dires :
« Elle avait affirmé qu'elle avait perdu sa montre de fitness en résistant à son agresseur, mais l'objet a été retrouvé intact dans le couloir, près de la salle de bains [où elle avait dit que s'était déroulé le viol, ndlr].
Selon le chef d'inculpation, quand les enquêteurs ont téléchargé son activité de fitness, ils se sont aperçus que la femme n'avait pas dormi cette nuit-là et qu'elle avait marché tout le temps, au lieu de dormir comme elle l'avait affirmé. »
En plus de ces données, les enquêteurs n'ont trouvé aucune trace de pas dans la neige autour de la maison (les faits se sont déroulés en mars) ni aucune trace d'intrusion. En conséquence, la femme a été inculpée pour fausse déclaration et altération de preuves.

Des grosses balances, ces Google Glass
Déjà, en novembre 2014, à Calgary (Canada), une femme, qui demandait à être indemnisée pour préjudice corporel après un accident, a utilisé les données de son bracelet connecté pour prouver que son activité physique était réduite depuis son accident. (Une histoire alors analysée par Olivier Ertzscheid.)

Les objets connectés arrivent donc dans les tribunaux. Et selon les avocats cités dans la presse américaine (ici ou ici, par exemple), cette tendance est appelée à grandir. Dans Wired, un avocat américain se demandait ainsi :
« [Les données des objets connectés] pourraient-elles être utilisées comme alibi ? »
Ou encore :
« Est-ce qu'on pourrait utiliser les données d'un FitBit pour prouver qu'un cardiologue avait fait preuve de négligence, en ne restreignant pas l'exercice d'un patient ? »
Ces objets peuvent donner des indications sur les activités de celui ou celle qui le porte, mais aussi sur le lieu où il ou elle se trouve, grâce à des fonctions de géolocalisation. Les plus sophistiqués, comme les Google Glass, font aussi des photos ou des vidéos, ainsi que des recherches sur le Web.
On voit bien l'usage que policiers, assureurs ou autres pourraient faire de ces données, en les retournant contre son propriétaire.

Bientôt dans nos prétoires
En France, le cas ne s'est encore jamais présenté, mais, explique Me Clarisse Le Corre, avocate au cabinet Vigo, il est tout à fait envisageable :
« Selon la loi, les infractions peuvent être établies par tous modes de preuve et c'est le juge qui décide ensuite selon son intime conviction. »
A cheval entre données personnelles et données médicales, ces informations sont souvent appelées « données de bien-être ». Elles sont protégées par la loi « Informatique et libertés », mais dans le cas d'un procès, cette protection peut être levée par l'instruction.
Pourvu qu'elles soient légalement recevables et qu'elles soient ensuite soumises au contradictoire, c'est-à-dire être débattues par les deux parties, les données des objets connectés peuvent tout à fait être présentées devant un tribunal.

Leurs données sont-elles fiables ?
Pourtant, ces données sont loin d'être totalement fiables.
Les objets connectés buguent.
Comme l'a récemment montré notre collègue Thibaut Schepman, les appareils connectés peuvent bugger et les données récoltées ne reflètent pas forcément vos activités.

Ils sont faciles à duper.
Pas besoin de réfléchir longtemps pour voir comment on pourrait duper le bracelet connecté : il suffit de le faire porter par un complice ou de l'apposer à un animal domestique au comportement pas trop erratique. Ou encore de rester assis à son bureau en bougeant les pieds très vite pour faire croire qu'on fait un jogging.

Ils « mesurent » selon des critères qui changent de machine en machine et sont déterminés par des algorithmes inaccessibles.
Comme le rappelle la chercheuse américaine Kate Crawford dans The Atlantic, les mesures qu'effectuent ces outils dépendent de la façon dont ils ont été programmés et sont souvent imprécises.

« Le Jawbone UP, Nike Fuelband, FitBit and Withings Pulses [différents modèles de bracelets connectés, ndlr] ont chacun des modes de fonctionnement particulier : certains comptabilisent les mouvements de bras comme de la marche (merveilleux, si vous voulez comptabiliser l'écriture comme de l'exercice), d'autres comptabilisent difficilement le vélo comme une activité physique.

La fonction de mesure du sommeil emploie des méthodes assez grossières pour faire la différence entre sommeil léger et sommeil profond. […] »

Un bracelet Jawbone Up (Ashley Baxter/Flickr/CC)

La chercheuse ajoute, faisant référence à l'exploitation de ces données :
« Ces données sont rendues encore plus abstraites par des entreprises d'analytique qui créent des algorithmes propriétaires, pour les comparer à leur standard de ce qu'est une personne normale "en bonne santé." »

Effectivement, explique Me Le Corre, à mesure que l'on s'interroge sur le statut de ces objets, on découvre leurs limites :

« La question de la fiabilité des données de ces objets va se poser de façon aiguë. Pour l'instant, nous manquons de recul sur ces choses-là parce qu'elles sont très récentes. D'où l'intérêt de le soumettre à la discussion des deux parties, qui sert de garde-fou. »

Les données par elles-mêmes ne signifient rien : elles s'intègrent dans un faisceau de preuves, et doivent toujours être contextualisées.

Au-dessus des témoins humains…
En voyant les données de bien-être utilisées contre leur propriétaire, on comprend aussi mieux ce que sont vraiment les objets connectés.
Ainsi, réfléchissant sur ce thème, la chercheuse Kate Crawford, qui travaille sur les implications du big data et des objets connectés, rappelle l'ambiguïté fondamentale des objets connectés :

– ils se présentent comme les instruments d'une meilleure connaissance de soi,
– mais sont aussi des « informateurs », qui collectent des données et les transmettent au fabricant et à des tiers – potentiellement à des assureurs et des employeurs.
[Plus profondément, c'est le statut que l'on veut donner à ces données qui est en jeu. Kate Crawford met en garde contre la tentation d'une « vérité fondée sur les données », où celles-ci finiraient par sembler plus fiables – parce que plus neutres – que l'expérience des témoins.

« Donner la priorité aux données, qui sont irrégulières et peu fiables, sur les témoignages humains, cela signifie que l'on donne le pouvoir à l'algorithme. Or ces systèmes sont imparfaits – comme peut l'être le jugement humain. »

Les données des objets connectées ne sont que ça, des données : des mesures qu'il faut contextualiser et comprendre, et surtout ne pas prendre pour argent comptant.

Source : http://rue89.nouvelobs.com/2015/07/01/quand-les-objets-connectes-temoignent-a-proces-contre-260040

Des chercheurs développent une étonnante attaque web sur la DRAM | Le Net Expert Informatique

Des chercheurs développent une étonnante attaque web sur la DRAM

Des chercheurs ont réussi à exploiter un défaut nommé « Rowhammer » qui inquiéte depuis longtemps les experts de la sécurité informatique. Leur attaque, menée depuis le web, s'appuie sur JavaScript et cible la DRAM des ordinateurs, exposant des millions d'internautes.

On sait depuis plusieurs années que les cellules mémoire des ordinateurs sont vulnérables à une interférence intentionnelle. Mais un récent document de recherche explique comment mener une attaque depuis le web qui augmente considérablement le danger pour les utilisateurs. Ce document, publié par des institutions autrichiennes et françaises – il a été coécrit par Daniel Gruss et Stefan Mangard de l'Université de Technologie de Graz en Autriche, et par Clémentine Maurice de Technicolor et Eurecom en France – pourrait obliger les fondeurs à trouver en urgence une solution qui résout le défaut connu sous le nom de « Rowhammer ».
Pour augmenter la densité de la DRAM, les concepteurs n'ont cessé de rapprocher les cellules, les rendant vulnérables aux interférences électriques. Une technique décrite sous le nom de « rowhammering » permet de changer la valeur binaire des cellules adjacentes en activant de manière répétée une rangée donnée de cellules de mémoire. Pendant longtemps, les concepteurs se sont préoccupés de la fiabilité posée par cette fuite électrique, sans considérer la question de la sécurité. Mais cette approche est en train de changer rapidement.

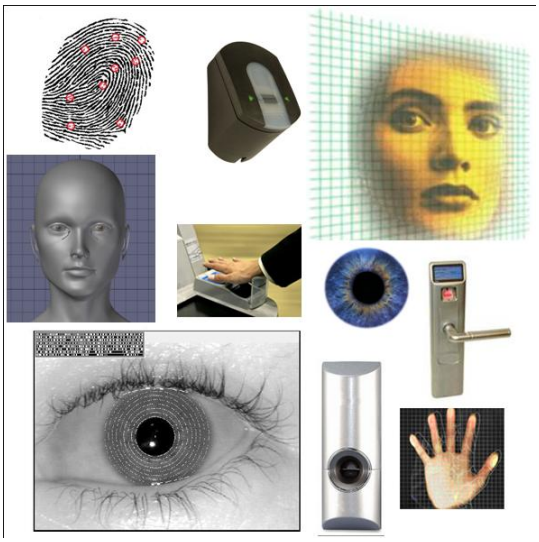
Une attaque à distance en JavaScript
Plus tôt cette année, des chercheurs de Google ont annoncé qu'ils avaient réussi à développer deux exploits opérationnels : le premier leur a permis de mener une attaque par escalade de privilège et l'autre utilise le changement de polarité induit par le défaut « Rowhammer » pour obtenir des privilèges au niveau du noyau. Mais, pour que l'attaque réussisse, ils avaient été obligés d'installer leurs exploits sur la machine de l'utilisateur. Ce qui est remarquable dans ce nouveau document, c'est qu'une telle attaque pourrait être menée depuis le web en s'appuyant sur JavaScript. Le code proof-of-concept Rowhammer.js a été testé dans Firefox 39, « mais notre technique d'attaque est générique et peut être appliquée avec tout type d'architecture, de langage de programmation et d'environnement runtime », ont-ils écrit. Elle ne nécessite pas un accès physique à un ordinateur, ce qui la rend beaucoup plus dangereuse.
Cela signifie également qu'un grand nombre de personnes pourraient être ciblées depuis le web, ce qui augmente le pool de victimes potentielles. « Étant donné que l'attaque peut être lancée simultanément et furtivement contre un nombre arbitraire de machines, elle représente une énorme menace pour la sécurité », ont-ils ajouté. De plus, un grand nombre d'ordinateurs sont vulnérables, puisque l'attaque est indépendante du système d'exploitation, et que le bug « Rowhammer » affecte de nombreux types d'architectures de puces. Les chercheurs essayent encore de savoir combien de systèmes seraient vulnérables à leur attaque. Jusqu'à présent, ils n'ont pas développé d'exploit qui permettrait d'obtenir un accès root à un ordinateur en exploitant le « rowhammering », mais ils pensent que des pirates pourraient éventuellement étendre les capacités de l'exploit qu'ils ont découvert.

Bloquer JavaScript avec NoScript
Tant que les fondeurs ne trouvent pas de solution à long terme pour résoudre le problème Rowhammer.js, les chercheurs proposent d'inclure dans les navigateurs web un test permettant de vérifier si l'ordinateur est vulnérable. Si le test est positif, « JavaScript doit être mis sous contrôle pour éliminer la possibilité d'un exploit. Même si le système est très probablement résistant, il faut laisser à l'utilisateur la possibilité d'activer explicitement JavaScript quand il visite une page web », écrivent-ils. Une autre alternative serait de désactiver complètement JavaScript en utilisant une extension comme NoScript. Mais de nombreux sites web reposent sur JavaScript et sans lui, la consultation de ces sites devient problématique.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-des-chercheurs-developpent-une-etonnante-attaque-web-sur-la-dram-61920.html
Par Jean Elyan et IDG NS

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 non 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 en sont, quant à eux, penchés sur le destin ou les forces libres en tant que mot de passe. Ils présenteraient notamment des atouts significatifs en matière de sécurité.

François Dominic Laramée dans un article de « Branches 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 investirait 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, ont 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 », mais 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 régaliens 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 « untraçable » 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 « désidentifiée » (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'État, 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.

Le 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-2242870.html
Par Atlantico et Jean-Paul Pinte

A quelles attaques informatiques doit-on s’attendre dans les mois qui viennent ? | Le Net Expert Informatique

A quelles attaques informatiques doit-on s’attendre dans les mois qui viennent ?

Brèches de sécurité et atteintes à la vie privée font régulièrement la une des journaux. Comment la course à l'armement entre les auteurs de cyberattaques et les spécialistes de la défense se développe t-elle ? Nous analysons dans cet article les prévisions des experts.

La sécurité des informations et le respect de la vie privée ont toujours été des sujets brûlants, mais cette année la température semble encore monter d'un cran. Ces derniers mois ont été marqués par des cyberattaques très médiatisées qui ont concentré l'attention du monde entier sur la protection des données, le cryptage, le respect de la vie privée et la surveillance, comme jamais auparavant. Ces événements ô combien médiatiques se déroulent sur fond de multiplication des fuites de données au niveau des gouvernements, des entreprises et autres organisations, familles et individus.
Nous avons examiné les articles prospectifs de 17 entreprises et attribué les 130 prévisions résultantes à un certain nombre de catégories émergentes pour produire le graphique ci-dessous.

Prévisions de sécurité de Blue Coat, Damballa, FireEye, Fortinet, Forrester, Gartner, IDC, ImmuniWeb, Kaspersky Lab, Lancope, McAfee, Neohapsis, Sophos, Symantec, Trend Micro, Varonis Systems et Websense.
Image : Charles McLellan/ZDNet
En tête de liste, figurent les « nouveaux vecteurs et plates-formes d'attaque » et « l'évolution des solutions de cybersécurité existantes », deux catégories qui illustrent la réalité de la course à l'armement en matière de cybersécurité.
Dans la première catégorie, plusieurs commentateurs ont souligné les « nouveaux bugs dans du code ancien largement utilisé » (Kaspersky Lab), tels que Heartbleed/OpenSSL et Shellshock/Bash. Sophos a noté des failles exploitables dans le protocole IPv6, ainsi que des capacités de robot et de rootkit dans l'environnement d'amorçage enrichi UEFI qui peuvent générer de nouveaux vecteurs d'attaque. Apple était la principale nouvelle plate-forme signalée, par exemple par FireEye, qui note que « étant donné qu'Apple est de plus en plus présent dans les entreprises, les concepteurs de programmes malveillants vont ajuster leur jeu d'outils ». Les récents chiffres de ventes record ne feront que creuser davantage l'appétit des pirates informatiques pour les produits d'Apple.

Source : http://www.zdnet.fr/actualites/cybersecurite-a-quoi-s-attendre-dans-les-mois-qui-viennent-39822112.htm
Par Charles McLellan

Boulanger, épinglé par la Cnil pour des commentaires sur un fichier client | Le Net Expert Informatique

Boulanger épinglé par la Cnil pour des commentaires sur un fichier client

La Cnil a mis en demeure la société Boulanger, dont les employés ont quelque peu abusé de l'espace libre laissé au sein d'un fichier client. Plusieurs commentaires insultants ont été constatés par la Commission, qui laisse 3 mois à la société pour se mettre en règle.

Peut-on inscrire n'importe quoi dans le champ commentaire d'un fichier client ? Pas vraiment : la Cnil a ainsi annoncé aujourd'hui avoir épinglé l'enseigne Boulanger suite à une plainte lui ayant signalé des commentaires injurieux dans ses fichiers clients.
Sur son site, la Cnil explique avoir effectué un contrôle sur place doublé d'un contrôle en ligne suite à un dépôt de plainte, qui lui a permis de constater des pratiques contrevenant à la loi Informatique et Libertés. « Les fichiers de la société comportaient de nombreux commentaires excessifs sur ses clients, comme par exemple « n'a pas de cerveau », « cliente avec problème cardiaque », « client alcoolique » ou encore des propos insultants » rapporte ainsi la Cnil, qui explique avoir mis en demeure Boulanger, sommé de se mettre en conformité avec la loi sous trois mois.

La Cnil veut faire un exemple
La Cnil explique avoir relevé pas moins de 5828 commentaires désobligeants parmi les fichiers clients de Boulanger. La société est également épinglée pour non-respect des règles encadrant l'usage des cookies : la société manquait à son obligation de prévenir l'utilisateur de l'utilisation de cookies pour le tracking et la Cnil relève également la mise en place « de certains cookies à finalité publicitaire [ayant] une durée de vie pouvant aller jusqu'à 15 ans. »
Pas de chance pour Boulanger, la Cnil explique avoir choisi de mettre en avant cette procédure « afin d'appeler notamment l'attention des entreprises sur la nécessité de ne pas enregistrer de commentaires excessifs dans leurs fichiers clients. » Il fallait faire un exemple et la Cnil précise que cette mise en demeure n'est pas une sanction, mais rappelle que si Boulanger ne se met pas en règle, une nouvelle procédure pourrait être initiée à l'encontre de Boulanger.Via son compte Twitter, la marque s'est excusé et promet de remédier à la situation.

Source : http://www.zdnet.fr/actualites/boulanger-epingle-par-la-cnil-pour-des-commentaires-sur-un-fichier-client-39822914.htm