Les voitures promises aussi à des bugs logiciels et des mises à jour ? | Le Net Expert Informatique

	Les voitures promises aussi à des bugs logiciels et des mises à jour ?

Ford doit rappeler 433.000 voitures en Amérique du Nord en raison d'un bug logiciel, à savoir l'impossibilité de couper le moteur. Les propriétaires doivent retourner chez leur garagiste pour effectuer une mise à jour. On n'arrête plus le progrès ?

Fin mai, Frédéric Charles du blog Green SI de ZDNet.fr expliquait pourquoi il avait été obligé rebooter sa voiture en raison d'un problème logiciel. Car en effet, le logiciel est de plus en plus présent dans nos véhicules. Pour les automobilistes, les pannes mécaniques ne sont plus le seul tracas qui les guette.
Et notre bloggeur n'est pas un cas isolé. Le constructeur Ford a ainsi été contraint d'émettre un rappel portant sur 433.000 voitures en Amérique du Nord (modèles Focus, C-MAX et Escape). C'est précisément le logiciel du système de commande qui est en cause.

Le logiciel apporte des fonctions, et des bugs potentiels
Sur son site Internet, Ford mentionne un dysfonctionnement du module de contrôle ayant pour conséquence l'impossibilité de couper le moteur de la voiture, y compris lorsque le conducteur tourne et retire la clé.
Les propriétaires concernés sont invités à se rendre chez leurs concessionnaires… afin d'appliquer une mise à jour logicielle sur leur véhicule, un peu comme cela se fait déjà, et depuis de nombreuses années, sur un ordinateur.
Confronté à l'impossibilité de reprendre la route, Frédéric Charles avait procédé à ce qui s'apparente à une forme de « reboot » ou redémarrage de sa voiture. Comment ?
« Clef dans la poche en dehors du véhicule, je débranche [la batterie], j'attends 30s, je rebranche, la voiture se réinitialise, je redémarre, et voilà que tout rentre dans l'ordre. Mon garagiste étant le premier surpris. J'ai depuis avalé des centaines de kilomètres sans aucun problème » racontait-il.
« L'enjeu des véhicules connectés est aussi le support numérique, de véhicules de plus en plus sophistiqués. Sinon, il ne nous restera plus qu'à apprendre à rebooter notre voiture régulièrement et croiser les doigts à chaque fois, comme avec les bon vieux PCs. Nostalgie, nostalgie… » commentait-il encore.

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

Source : http://www.zdnet.fr/actualites/les-voitures-promises-comme-les-pc-a-des-bugs-logiciels-et-des-mises-a-jour-39822008.htm

Des communications ultra-sécurisées avec TEOREM | Le Net Expert Informatique

Des communications ultra-sécurisées avec TEOREM

TEOREM est un système de téléphonie mobile et fixe à usage gouvernemental et de Défense. Il permet de protéger les communications vocales ainsi que les SMS sur tous les réseaux opérateurs. TEOREM assure également le rôle de modem chiffrant permettant ainsi l'échange de données entre deux ordinateurs personnels en toute sécurité.

Grâce à sa parfaite interopérabilité avec les différents réseaux de télécommunication fixes (analogiques et numériques) et mobiles (2G / 3G), TEOREM offre une grande polyvalence aux utilisateurs. Enfin, son autonomie, sa miniaturisation et sa grande flexibilité en font une solution unique pour répondre aux besoins des utilisateurs nomades.

Une solution hautement sécurisée et simple d'utilisation :
• Configuration fixe ou mobile (2G / 3G).
• Certifiée jusqu'au niveau Secret Défense pour la France.
• Communications sécurisées de bout en bout.
• Signal lumineux permettant de différencier les appels sécurisés et non sécurisés.

Un système flexible et performant :
• Compatible avec les réseaux d'opérateurs et gouvernementaux.
• Système de gestion centralisé à distance.
• Gestion sans intervention de l'utilisateur final.
• Grande qualité audio : + 15%* comparé aux téléphones standards.

* Selon norme PESQ.

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

Source : https://www.thalesgroup.com/fr/cybersecurite/teorem

Une imprimante 3D pour personnaliser la mousse de votre café latte | Le Net Expert Informatique

	**Une imprimante 3D pour personnaliser la mousse de votre café latte**

Un support de communication inattendu développé par la startup Coffee Ripples.

L'entreprise Coffee Ripples a mis au point une machine qui permet d'écrire le message de votre choix sur la mousse d'un café : The Ripple Maker. Un site et une app mobile permettent d'uploader et adapter le message désiré. Celui-ci est alors imprimé sur la surface de la boisson en poudre de café, combinant ainsi les technologies de l'impression 3D et du jet d'encre. Coffee Ripples mise sur un prix de vente de 999 USD avec un abonnement annuel de 75 USD pour permettre aux commerces d'utiliser pleinement toutes les fonctionnalités et s'attirer le capital sympathie des clients. Retrouvez plus d'information sur le site de de la startup.
Coffee Ripples profite ainsi d'un emplacement peu investi pour communiquer, tout en surfant sur un art de plus en plus populaire. Il suffit pour cela de jeter un œil au hashtag #latteart sur Instragram. Lufthansa a d'ores et déjà signé pour cette technologie dans le but d'imprimer le logo de la compagnie sur les cafés des voyageurs de première classe.

Source : http://lareclame.fr/132138-coffee-ripples-un-cafe-pour-instagram-sans-filtre

Reconnaissance faciale, une menace pour la vie privée ? | Le Net Expert Informatique

Pour le «Washington Post», les nombreuses applications capables de reconnaître les visages créent des bases de données biométriques dangereuses pour la «confidentialité numérique».

«L'anonymat en public pourrait être une chose du passé.» Dans le Washington Post du 11 juin, Ben Sobel, chercheur au Centre sur la vie privée et la technologie de l'école de droit de Georgetown, consacre un article au risque qui pèse sur notre «confidentialité biométrique». Selon lui, les technologies de reconnaissance faciale se développent à la vitesse grand V sous l'impulsion du marketing individualisé. Et pas toujours de manière très légale…

Aux Etats-Unis, Facebook fait l'objet d'un nouveau procès en action collective, concernant la violation du droit à la protection des données personnelles de ses utilisateurs. En cause, le réseau social serait en train de créer «la plus grande base de données biométriques privées au monde» sans demander assez explicitement le consentement de ses utilisateurs comme l'explique le site Sophos. Le gouvernement américain et le département du Commerce auraient déjà invité des associations de défense de la vie privée ainsi que des représentants des grandes entreprises de ce secteur comme Google et Facebook pour essayer de réglementer l'usage de ces technologies.
Mais pour le moment, seul l'Illinois (2008) et le Texas (dès 2001) ont des lois interdisant l'utilisation de cet outil sans le «consentement éclairé» des utilisateurs, explique Ben Sobel. Selon lui, l'issue de ce procès, qui devra déterminer si Facebook a enfreint la «Biometric Information Privacy Act» (BIPA) de l'Illinois, déterminera l'avenir des applications de reconnaissance faciale sur le marché. Il encourage ainsi les Etats-Unis à adopter une loi fédérale pour garantir la «confidentialité biométrique» des Américains.

LE BOOM DES APPLICATIONS DE RECONNAISSANCE FACIALE
FaceNet (Google), Name Tag (FacialNetwork) ou encore Moments (Facebook). Toutes ces applications utilisent des algorithmes de reconnaissance faciale. Et pour les imposer sur le marché, les entreprises sont prêtes à tout pour mettre leur adversaire échec et mat.
FaceNet, la technologie développée par le géant Google, possède une précision de 99,63 % selon Ben Sobel. Elle est actuellement utilisée par Google Photos dans ses versions non européennes. Dans la même lignée, Name Tag, développé par FacialNetwork, ambitionne de fonctionner sur les Google Glass. Cette application permettrait de rassembler tous les profils sur les réseaux sociaux disponibles sur Internet (Twitter, Instagram, Google+ et sites de rencontres américains) selon un article du Huffington Post. Une application qui pourrait permettre d'avoir le profil social de quelqu'un en temps réel.
Parmi les fonctionnalités envisagées, il y aurait par exemple celle de révéler la présence de quelqu'un dans les bases de données criminelles. Pour le moment, Google a refusé que NameTag soit disponible sur ses Google Glass, pour des questions de problèmes de respect de la vie privée… Mais il n'est pas le seul à s'engouffrer dans ce marché.
Depuis 2011, Facebook utilise un système de suggestion de tags (identifications) sur les photos. Bien qu'interdit en Europe, Deepface, l'algorithme expérimental du réseau social, serait capable de reconnaître les gens à leur posture corporelle. De fait, son algorithme utilise ce que l'on appelle des «poselets». Inventés par Lubomir Bourdev, ancien chercheur de Berkeley œuvrant désormais chez Facebook IA Research. Ceux-ci repèrent les caractéristiques de nos visages et trouvent ce qui nous distingue de quelqu'un d'autre dans une pose similaire, explique un article de Numérama (http://www.numerama.com/magazine/33026-meme-de-dos-facebook-sait-vous-reconnaitre-sur-les-photos.html). Mais Facebook ne s'arrête pas là. En juin, le réseau social a présenté Moments, une application permettant de partager de manière privée des photos avec des amis utilisant elle aussi une technologie de reconnaissance faciale. D'ores et déjà disponible gratuitement aux Etats-Unis, elle permet à un utilisateur d'échanger avec ses amis des photos où ils figurent de manière synchronisée. Une vidéo en explique les rouages :

Moments ne devrait pas s'exporter en Europe de sitôt, puisque l'UE exige la mise en place d'un mécanisme d'autorisation préalable qui n'est pas présent sur la version américaine. Et ce, bien que les utilisateurs puissent désactiver les suggestions d'identification sur les photos, via les paramètres de leur compte.

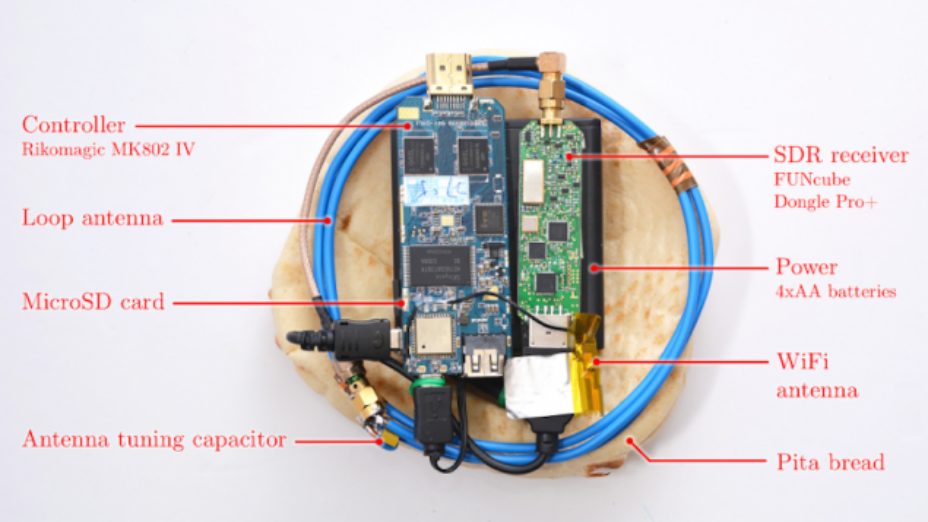
L'INQUIÉTUDE AUTOUR DU SUCCÈS DE CES TECHNOLOGIES
En 2012, une recommandation formulée par le G29, qui réunit les commissions vie privée de 29 pays européens, mettait déjà en garde contre les dangers de la reconnaissance des visages sur les médias sociaux. Notamment concernant les garanties de protection des données personnelles, tout particulièrement les données biométriques. Pour le moment relativement bien protégés par la législation européenne, nous ne sommes pas pour autant épargnés par ces outils.

Tous les jours, 350 millions de photos sont téléchargées sur Facebook, selon Ben Sodel. Or, le public semble majoritairement insouciant face à la diffusion de son identité (nom, image…), souligne InternetActu. A l'exemple de l'application How Old mise en ligne fin avril, qui se targue de deviner votre âge grâce à une photo. Corom Thompson et Santosh Balasubramanian, les ingénieurs de Microsoft à l'origine du projet, ont été surpris de constater que «plus de la moitié des photos analysées» par leur application n'étaient pas des clichés prétextes mais de vraies photos, rapporte le Monde.

Mais le succès (bien qu'éphémère) de cette application démontre bien que le public n'est pas vigilant face à la généralisation de la reconnaissance faciale. Un peu comme avec la diffusion des données personnelles au début de Facebook. Il ne s'agit pas tant du problème de stocker des photos d'individus que de mémoriser l'empreinte de leur visage. Entre de mauvaises mains, ces bases de données pourraient mettre à mal notre «confidentialité biométrique».

Source : http://ecrans.liberation.fr/ecrans/2015/06/26/reconnaissance-faciale-une-menace-pour-la-vie-privee_1337015
Par Camille PETTINEO

Pour pirater un ordinateur, une pita suffit | Le Net Expert Informatique

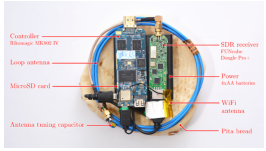


Pour pirater un ordinateur, une pita suffit

Selon une étude de l'université de Tel-Aviv, travailler dans un café pourrait s'avérer risqué pour la sécurité de votre ordinateur

Cette pita, qui donne l'apparence innocente que quelqu'un mange ostensiblement en face de vous dans le café de votre quartier, pourrait contenir un système d'espionnage informatique pouvant infiltrer les protocoles d'encodage les plus sécurisés de votre ordinateur.

Pire encore, ont déclaré les chercheurs de l'Université de Tel-Aviv, les utilisateurs de cet ordinateur ne peuvent pas faire grand chose pour se protéger.
« Des techniques d'atténuation… pourraient inclure des cages Faraday », des écrans en métal spécialement posés au sol qui bloquent les radiations… « Pourtant, la protection peu chère de PC de niveau commercial semble difficile », explique l'équipe.
Dans un article publié mardi, les chercheurs décrivent le très faible coût de l'équipement de type Radio Shack, que l'on peut facilement cacher dans un pain pita standard et qui peut être utilisé pour « lire » des impulsions électromagnétiques provenant du clavier d'un ordinateur standard, y compris les frappes sur le clavier afin de décrypter les documents sécurisés.
De manière amusante, l'Université de Tel-Aviv a appelé l'attaque PITA, Instrument portable pour l'acquisition de signaux.



L'étude, menée par les chercheurs Daniel Genkin, Itamar Pipman, Lev Pachmanov et Eran Tromer a été publiée pour coïncider avec une conférence majeure de sécurité informatique qui va avoir lieu à l'Université de Tel-Aviv (UTA) cette semaine.
« Nous avons pris avec succès des codes d'ordinateurs de divers modèles fonctionnant avec GnuPG (une source populaire d'encodage, en utilisant le standard d'encodage OpenPGP) en quelques secondes », a écrit l'équipe de l'UTA dans l'article, intitulé « Voler des codes de PC en utilisant une radio : des attaques électromagnétiques à moindre coût sur une exponentiation de fenêtres ».
En plus d'OpenPGP, l'équipe a été capable de dupliquer avec réussite les attaques sur d'autres systèmes d'encodages, très sécurisés, y compris RSA et ElGamal.
« L'attaque envoie quelques textes informatiques bien conçus et lorsque ces textes sont décryptés par la cible, ils entraînent l'occurrence de valeurs spécialement structurées dans le logiciel d'encodage », ont déclaré les chercheurs.
En utilisant un appareil qui peut recevoir des signaux radio, une simple radio ou une clé USB pouvant recevoir des émissions et les lire sur l'ordinateur, les chercheurs ont été capables d'observer les fluctuations dans le champ électromagnétique entourant l'ordinateur et de traduire ces fluctuations en frappes de clavier en utilisant un programme d'analyse.
L'article fournit des détails complets sur l'équipement nécessaire (tout est disponible et peu cher dans un magasin local d'électronique ou sur Internet), et sur la façon d'assembler et de connecter les parties, et même de les plier dans un pain pita.

L'équipement détecte les fluctuations dans le champ électromagnétique émis par le matériel informatique (clavier et processeur) lorsque l'ordinateur essaie de décrypter les signaux (les modules d'encodage contiennent des composants qui peuvent être exploités pour fonctionner automatiquement lorsque le texte encodé est rencontré).

En envoyant ces textes pièges, les pirates peuvent voler les codes d'authentification sur l'ordinateur de l'utilisateur, leur autorisant un accès libre aux documents et aux données encodés.

Une attaque PITA pourrait probablement être utilisée par des pirates en cas d'une attaque qui « balaie » des données et les documents d'un ordinateur.

Si ces données sont encodées, il est peu probable que les pirates pourront les lire (en fonction de niveau de complexité du codage), mais avec des clés d'encodage, les pirates pourraient trouver des informations encodées comme des numéros de cartes de crédit ou des mots de passe.

La seule mise en garde est que la pita « espion » a besoin de se trouver à 50 centimètres de la cible.

Mais d'après l'équipe, la totalité de l'opération peut être réalisée en quelques secondes, rendant l'attaque parfaite pour les pirates dans les cafés où de nombreux utilisateurs d'ordinateurs profitent des installations électroniques, du wifi et de boissons pour travailler.

Un pirate pourrait obtenir les codes dans une attaque « en marchant », attaque menée en transportant une « pita empoisonnée » sur un plateau avec de la vraie nourriture. L'étude notait pourtant que la « qualité du signal variait fortement en fonction du modèle de l'ordinateur cible et de la position de logiciel espion ».

L'équipe de UTA n'est pas la première à penser à utiliser des impulsions électromagnétiques pour pirater des systèmes.

En 2014, des chercheurs de l'Université Ben Gourion (UBG) ont pu utiliser un programme pirate sur un téléphone portable pour collecter des radiations électromagnétiques provenant de claviers, de moniteurs et d'autres équipements pour lire des informations importantes.

L'équipe de l'UBG a démontré comment les données collectées par le programme espion, auparavant placé sur un ordinateur (à travers une attaque de phising ou une autre méthode), pouvaient être captées par un téléphone portable qui créait un réseau local en utilisant des impulsions émanant de matériel informatique.

Les informations du système cible pouvaient être captées, même s'il n'est pas connecté à internet ou à un réseau local (Ethernet).

Le pire, a déclaré l'équipe, est qu'il n'y a pas grand chose que les utilisateurs d'ordinateur puissent faire pour éviter ces attaques, si ce n'est éviter les cafés et garder leur ordinateurs loin des pitot.

Malheureusement, l'équipe a déclaré « qu'empêcher la fuite à un bas niveau de prévention est presque impossible » parce que mettre en place des mesures efficaces (comme des cages Faraday) serait très gênant à cause du matériel informatique excessif ou ralentirait la capacité au point que les utilisateurs seraient incapables d'accomplir le moindre travail.

« Même lorsqu'un programme cryptographique est sûr mathématiquement, ses mises en place peuvent être vulnérables à des attaques de réseaux secondaires qui exploitent des émanations physiques », a déclaré l'équipe. Le pirate « peut facilement viser les ordinateurs ».

« Nous avons testé de nombreux ordinateurs de modèles variés », et lorsqu'il s'agit d'une attaque PITA, chaque utilisateur d'ordinateur devrait se sentir concerné.

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

Source : http://fr.timesofisrael.com/pour-pirater-un-ordinateur-une-pita-suffit/
Par David Shamah

La Gendarmerie Nationale souhaite s'équiper d'une vingtaine de drones | Le Net Expert Informatique

La Gendarmerie Nationale souhaite s'équiper d'une vingtaine de drones

La Gendarmerie nationale souhaite s'équiper d'une flotte de drones, comme l'avait récemment annoncé Bernard Cazeneuve. Et c'est un appel d'offres qui a été lancé pour l'achat d'une vingtaine de drones répondant à certains critères spécifiques.

Le ministère de l'Intérieur vient de lancer un appel d'offres visant » la fourniture de microdrones au profit de la Gendarmerie nationale, le maintien en condition opérationnelle des microdrones acquis, et la formation pour la fonction de télépilote ». Plus qu'une flotte de drones, il est question des dispositifs ainsi que d'une formation à leur utilisation et leur entretien.
La Gendarmerie nationale devrait disposer de 23 appareils de la famille des « quadrirotors à décollage vertical » qui permettent un contrôle précis, une stabilité accrue, mais qui permettront le vol stationnaire pour la mise en place d'opération de surveillance.
Il sera question de 4 à 6 drones haut de gamme qui devront disposer d'un mode de vol manuel et automatique. Le drone devra être capable de voler tout seul selon un ensemble de points de passage prédéfini. Son autonomie devra être d'au moins 20 minutes avec une vitesse équivalente à un kilomètre avalé en moins de deux minutes. L'appareil devra embarquer une caméra et retransmettre ses images en direct.
Un second lot de 19 à 30 drones sera constitué de modèles plus accessibles. La Gendarmerie nationale souhaite toujours un mode de vol automatique ainsi qu'une caméra embarquée, mais ici, la question de l'autonomie et de la vitesse importent moins, puisqu'il s'agira avant tout de mener des opérations de surveillance fixe dans le cadre d'interventions de sécurisation de la voie publique.
La Gendarmerie nationale souhaite des drones fiables, équipés de zoom x10 au minimum, le tout avec un relatif silence opérationnel permettant la mise en place d'une surveillance discrète.

Source : http://www.generation-nt.com/gendarmerie-nationale-equipe-drones-volants-actualite-1916394.html

Quelques conseils pour préserver votre e-réputation | Le Net Expert Informatique

Quelques conseils pour préserver votre e-réputation

Sur le web, rien ne se perd. Toutes les données qui vous concernent sont potentiellement accessibles par tous. Qu'il s'agisse des photographies de votre vie étudiante festive, des archives du blog que vous aviez tenu lors d'un voyage à l'étranger, de votre participation sur la liste électorale d'un parti politique sulfureux lors d'élections locales ou encore du jugement relatant une condamnation pénale : vous laissez des traces.

Celles-ci peuvent se révéler encombrantes. Comment faire pour qu'elles soient déréférencées des moteurs de recherche et ainsi rendues inaccessibles ?

Tout d'abord, il peut être utile de consacrer quelques minutes au paramétrage de la confidentialité de son compte sur les réseaux sociaux, afin de préserver le caractère privé de ses publications. Celles-ci ne seront alors pas accessibles par le biais des moteurs de recherche mais réservées à vos amis et relations.

Dans le cas où le contenu visé est publié sur un site web tiers, tel qu'un éditeur de presse, un blog ou un forum de discussion, il est possible de demander sa suppression en s'adressant directement à l'éditeur du site concerné ou, lorsque celui-ci ne réagit pas ou n'a pu être identifié, à l'hébergeur (qui assure le stockage du site sur ses serveurs).

En cas d'échec de cette démarche, les moteurs de recherche pourront être sollicités au titre du droit à l'oubli, par le biais des différents formulaires qu'ils proposent désormais [1].

Les principaux refus opposés par les moteurs de recherche sont justifiés par le fait que l'information litigieuse est toujours d'actualité, qu'elle ne concerne pas une personne physique, que l'internaute est un personnage public ou que le plaignant est un personnage public.

En dernier recours, le Tribunal compétent pourra être saisi. Attention toutefois, le juge saisi analyse en détail la demande présentée afin de s'assurer qu'elle ne porte pas atteinte à la liberté d'information du public. Ainsi, le Tribunal de grande instance de Paris a rejeté une demande de suppression et de désindexation d'un article en ligne du quotidien 20 Minutes [2]. L'article litigieux, accessible sur le site internet du quotidien, intitulé « Un cavalier accusé de viol », relatait le placement en garde à vue d'un cavalier de niveau international soupçonné d'être impliqué dans le viol d'une stagiaire.

Les juges ont rejeté la demande de droit à l'oubli, en faisant prévaloir la liberté d'information et l'intérêt légitime à divulguer des informations visant une personne exerçant une profession faisant appel au public et encadrant une activité proposée, notamment, à des enfants.

Au contraire, dans une décision précédente, la même juridiction avait ordonné à la société Google de retirer de ses résultats de recherche un lien vers un article du Parisien évoquant la condamnation, datant de 2006, d'une internaute pour escroquerie à une peine de trois ans de prison dont trois mois fermes. La plaignante, à la recherche d'un emploi, s'était tournée vers la Justice à la suite du refus préalablement opposé par le géant américain.

Lorsque votre demande est rejetée par le tribunal saisi, il reste possible de faire appel à des structures spécialisées qui tenteront de renvoyer au-delà de la troisième page de résultats, le contenu qui vous gêne.

A l'heure où de plus en plus de plateformes proposent aux internautes de redevenir propriétaires de leurs données personnelles et de gagner de l'argent en louant leurs profils [3] aux marques et annonceurs, il est plus que jamais important de permettre aux internautes de retrouver la maîtrise de leur e-réputation.

Source : http://www.village-justice.com/articles/Quelques-conseils-pour-preserver,19708.html

Un centre de compétence Kaspersky doit être mis en place très prochainement au Gabon | Le Net Expert Informatique

Un centre de compétence Kaspersky doit être mis en place très prochainement au Gabon

Un centre de compétence Kaspersky doit être mis en place très prochainement au Gabon, selon les termes d'un accord de partenariat signé mardi à Libreville entre l'Agence nationale des infrastructures numériques et des fréquences (Aninf) et l'éditeur Kaspersky.

En vertu de cet accord, signé par le directeur général de l'Aninf, Alex Bernard Bongo Ondimba et le vice-président de Kaspersky, Veniamin Levtsov, le futur centre, qui aura, par ailleurs, une vocation sous régionale, doit permettre au Gabon d'assurer la veille, la détection, l'analyse et la prévention des cyber-attaque.

« Ce partenariat est très salutaire pour le Gabon du fait qu'il nous permettra de nous doter d'un véritable système de défense en matière de virus et en ce qui concerne la cybercriminalité », a déclaré M. Alex Bernard Bongo Ondimba.

Outre la mise en place d'un centre de compétence au Gabon, l'accord signé porte également sur le transfert des compétences dans les domaines de la sécurité industrielle et de la cybercriminalité.

'Nous entendons contribuer à sauver le monde en mettant en place des systèmes de lutte contre des attaques axées sur la cybercriminalité. Nous voulons également apporter nos compétences aux structures locales », a affirmé, pour sa part, M. Levtsov.

Implantée dans plusieurs pays d'Afrique et dans d'autres continents, Kasperky est une entreprise russe leader mondiale en matière de sécurité informatique.

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

Source :
https://mail.google.com/mail/u/0/?hl=fr&shva=1#inbox/14e3b659f932c0fd?compose=14e2eb99aeedd11a

La première soirée Implant Party débarque à Paris | Le Net Expert Informatique

	La première soirée Implant Party débarque à Paris

La première « implant party » française a été organisée à Paris dans le cadre de l'opération Futur en Seine à La Gaîté Lyrique. Le concept, se faire implanter une puce sous la peau pour différentes applications du quotidien.

Sommes-nous en train d'assister à un tournant dans le domaine de l'interface homme/technologie ? Jusqu'à maintenant (sauf cas extrême), les modifications corporelles se cantonnaient aux tatouages, aux piercings ou écarteurs et à la chirurgie esthétique.
Mais depuis quelques mois, une nouvelle tendance née dans les pays scandinaves devient de plus en plus populaire, les Implant Party. Un concept qui consiste à se faire implanter une puce NFC sous la peau et permettre à son porteur d'interagir avec de nombreuses technologies de notre quotidien.

Une puce NFC sous la peau
Ce weekend, Paris a accueilli sa première implant party dans le cadre de l'opération Futur en Seine à La Gaîté Lyrique. Chacun pouvait venir se faire implanter une puce NFC par un spécialiste formé à cette opération.
Bien entendu, pas question de faire n'importe quoi et l'opération, facturée 200 euros, est effectuée dans des conditions d'hygiène drastiques et dans un environnement totalement stérilisé. Le biohacker (nom donné à la personne qui reçoit l'implant) se voit injecter une puce NFC grosse comme un grain de riz sous la peau après une anesthésie locale. Une fois l'opération effectuée, il devient possible pour le porteur de la puce d'interagir sans contact avec les équipements NFC qui l'entoure.

Des applications multiples, notamment dans le domaine professionnel
Déverrouiller son smartphone, ouvrir une porte, allumer un ordinateur ou encore payer un petit achat du quotidien d'un simple geste de la main, voilà ce que permet la technologie implanté dans le biohacker.
Ce mouvement d'un nouveau genre a été créé en Suède par l'association à but non lucratif Bionyfiken. 400 salariés suédois se sont récemment vus proposer la possibilité de se faire implanter une puce NFC pour entrer dans leurs locaux, payer leur repas ou faire des photocopies. Si jamais le biohacker regrette son acte, il est possible de se faire enlever la puce.

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

Source : http://www.begeek.fr/les-implant-party-debarquent-a-paris-172890

Compter une population seulement avec le Wi-Fi | Le Net Expert Informatique

Compter une population seulement avec le Wi-Fi

Plus besoin de se baser sur le nombre de smartphones connectés dans une certaine zone pour compter des groupes de personnes. La découverte de chercheurs de Santa Barbara se base uniquement sur le signal Wi-Fi.

L'idée est assez simple sur le papier : analyser les variations des ondes Wi-Fi d'une certaine zone pour compter les personnes présentes. Partant du principe que chacun altère légèrement les ondes par sa présence, les chercheurs de l'université de Californie Santa Barbara ont mis au point un modèle mathématique pour estimer le nombre d'individus dans une zone donnée. Le professeur d'ingénierie informatique Yasamin Mostofi et son équipe ont disposé deux spots Wi-Fi à deux extrémités d'une aire de 70 mètres carrés. Grâce à l'analyse de leurs ondes, les ingénieurs sont ensuite parvenus à estimer le nombre de personnes présentes dans la zone en temps réel. Et ce même si les individus étaient en mouvement.

Un outil pour la sécurité ?

En fait, la découverte répond à un besoin : celui de connaître l'étendu d'un groupe de personnes dans une manifestation ou dans un lieu public. La sécurité de certains événements pourrait en être accrue, selon les chercheurs, grâce à la notion de temps réel qu'apporte l'invention, même si les méthodes de comptage par les données télécoms se rapprochent déjà de ces objectifs. D'autant que le Wi-Fi ne peut s'étendre sur une surface aussi large que celles qui voient défiler des manifestants. L'aspect sécuritaire ne concernerait donc que les petits événements. Son seul avantage étant la prise en compte des individus sans smartphone.

Le Wi-FI rendra-t-il les bâtiments plus verts et plus intelligents ?

Vers des bâtiments plus intelligents

C'est en réalité dans un autre domaine que la découverte pourrait changer la donne. Les bâtiments intelligents seraient, en effet, à même de bénéficier d'une telle invention. Comme l'explique le professeur Mostofi dans le communiqué de l'université : « les stores intelligents pourraient se servir du dénombrement des utilisateurs du lieu pour mieux s'adapter par exemple ». Savoir précisément le nombre d'occupants d'un lieu ou le nombre de consommateurs dans un magasin permettrait à la fois une consommation d'énergie plus efficace mais également une nouvelle opportunité marketing. Les écrans publicitaires pourraient, en effet, se moduler selon la population présente pour ne citer que cet exemple.

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

Source :
http://www.atelier.net/trends/articles/compter-une-population-seul-wi-fi_436129?utm_source=emv&utm_medium=mail&utm_campaign=lettre_toute_zone