L’évolution De La Carte SIM

	L’évolution De La Carte SIM

Une carte SIM, ou Suscriber Identity Module en anglais (module d'identification de l'abonné), est un élément familier d'un téléphone portable. Elle peut facilement être échangée ou remplacée, mais elle n'est néanmoins pas née en même temps que le téléphone portable. Les premiers téléphones portables ne permettaient que des normes de communication « intégrées » : les paramètres de souscription étaient codés en dur dans la mémoire du terminal mobile.

Les normes analogues les plus anciennes comme NMT-450 n'utilisaient aucune sécurité : les données d'abonnement pouvaient être copiées sur un autre appareil et clonées, ce qui permettait d'appeler et d'accepter des appels au nom du propriétaire légitime sans payer.

Le premier dispositif de sécurité, inventé un peu plus tard, fut le code SIS, Suscriber Identity Security en anglais (sécurité de l'identité de l'abonné) : il s'agissait d'un nombre à 18 chiffres unique à chaque appareil et codé en dur dans un processeur d'application. Les codes SIS étaient répartis entre les fournisseurs de manière à ce que deux appareils ne puissent pas partager le même code SIS. Le processeur comportait également un code RID de 7 chiffres qui était transmis à une station de base lorsqu'un abonné s'inscrivait dans un réseau mobile.

La station de base générait un nombre aléatoire que le processeur SIS utilisait couplé avec une réponse SIS unique pour produire la clé d'autorisation.

Les clés et les nombres étaient relativement courts, mais appropriés pour l'année 1994 ; de façon assez prévisible, le système a été décrypté plus tard, tout juste trois ans avant l'apparition de la norme GSM, Global System for Mobile en anglais (Communications – Système global pour les communications mobiles). Il était conçu de manière plus sûre étant donné qu'il utilisait un système d'autorisation similaire, mais au chiffrement plus résistant. Ainsi, la norme est devenue « détachée » .

Cela signifie que l'autorisation dans sa totalité avait lieu sur un processeur externe intégré dans une carte intelligente. La solution a été appelée SIM. Avec l'introduction des cartes SIM, l'abonnement ne dépendait plus l'appareil et l'utilisateur pouvait changer d'appareil aussi fréquemment qu'il le désirait tout en gardant son identité mobile.

Fondamentalement, une carte SIM est une carte intelligente selon la norme ISO 7816, qui ne présente pas de différence significative par rapport à d'autres cartes intelligentes de contact comme les cartes de crédit ou les cartes téléphoniques. Les premières cartes SIM faisaient même la taille d'une carte de crédit, mais la tendance globale de réduction des dimensions a mené à une nouvelle forme plus compacte.

Les cartes SIM traditionnelles 1FF (1st Form Factor) de taille complète ne rentraient plus dans les téléphones, et l'industrie a donc trouvé une solution de compatibilité simple : une carte SIM plus petite (mini-SIM, 2FF ou 2nd Form Factor) qui est commune pour les utilisateurs modernes, a été placée dans un support en plastique de taille 1FF afin que la nouvelle forme de carte comporte la puce et les contacts, mais avec une empreinte plus petite, et puisse facilement être sortie.

Bien que cette tendance à la réduction continue avec la micro-SIM (3FF) puis la nano-SIM (4FF) , la forme et les contacts ainsi que les fonctionnalités de ces puces intégrées n'ont pas changé depuis presque 25 ans. De nos jours, de grands supports en plastique sont produits pour répondre aux besoins des utilisateurs qui préfèrent encore des combinés à l'ancienne.

Ceci dit, de nombreux appareils obsolètes ne supporteraient pas les cartes SIM actuelles, même dans leur version complète. Cela vient du fait que la tension de fonctionnement était de 5 V dans les anciennes cartes SIM alors que les actuelles exigent 3 V. De nombreux fabricants de SIM préfèrent sacrifier la compatibilité pour réduire les coûts, et la majorité des cartes SIM modernes ne supporteraient donc pas deux tensions. C'est pour cela que dans un ancien téléphone uniquement compatible avec 5 V, les cartes SIM de seulement 3V ne fonctionneraient même pas à cause de la protection de la tension de leur processeur.

Lors de la production, certaines informations sont écrites dans la mémoire d'une carte SIM : l'IMSI (International Mobile Suscriber Identity, Identité de l'abonné mobile international), en accord avec le porteur ayant commandé la carté, ainsi qu'une clé de 128 bits nommée Ki (Key Identification, identification de clé). Pour résumer simplement, on peut dire que l'IMSI et le Ki sont le l'identifiant et le mot de passe respectifs de l'abonné codés en dur dans la puce de la carte SIM.

La correspondance entre l'IMSI d'un abonné et son numéro de téléphone est stockée dans une base de données spéciale appelée HLR (Home Location Register). Ces données sont copiées sur une autre base de données, VLR (Visitor Location Register) dans chaque segment du réseau, sur la base de l'enregistrement temporaire de l'abonné en tant qu' « invité » sur une autre station de base.

Le processus d'autorisation est relativement simple. Lorsqu'un abonné est inscrit dans la base de données temporaire, VLR envoie un numéro de 128 bits aléatoire (RAND) au numéro de téléphone. Le processeur de la carte SIM utilise l'algorithme A3 pour créer une réponse de 32 bits (SRES) au VLR basé sur le numéro RAND et le Ki. Si VLR obtient une réponse qui correspond, l'abonné est inscrit dans le réseau.

La SIM crée également une autre clé temporaire appelée Kc. Sa valeur est calculée sur la base du RAND et du Ki mentionnés ci-dessus, à l'aide de l'algorithme A8. Cette clé est ensuite utilisée à son tour pour chiffrer des données transmises par l'algorithme A5.

Les noms de tous ces acronymes peuvent paraître un peu compliqués, mais l'idée de base est très simple : vous avez tout d'abord un identifiant et un mot de passe codés en dur dans la SIM, puis vous créez des clés de vérification et de chiffrement avec quelques trucs mathématiques et ça y est : vous êtes connecté !

Ce chiffrement est toujours activé par défaut, mais dans certaines circonstances (par exemple si un mandat est fourni), il peut être désactivé, ce qui permet qu'une agence de renseignement puisse intercepter les conversations par téléphone. Dans ce cas, les anciens dispositifs affichaient un cadenas ouvert, alors que les téléphones modernes (à part Blackberry) n'affichent aucune indication de ce type.

Il existe une attaque spécifiquement conçue pour intercepter les conversations téléphoniques ; pour la réaliser, l'adversaire a seulement besoin d'un appareil appelé IMSI Catcher qui imite une station de base et enregistre les téléphones qui se connectent avant d'envoyer tous les signaux vers une station de base réelle.

Dans ce cas, tout le processus d'autorisation se déroule de façon normale (il n'est pas nécessaire de décrypter les clés de chiffrement), mais la fausse station de base ordonne au dispositif de les transmettre sous forme de texte brut afin qu'un adversaire puisse intercepter les signaux sans que la compagnie ou l'abonné ne le sachent.

Cela peut paraître étrange, mais cette vulnérabilité n'en est pas vraiment une : en fait, cette fonctionnalité a été conçue pour faire partie du système depuis le début, afin que les services de renseignements puissent réaliser des attaques intermédiaires dans les cas appropriés… [Lire la suite]

Réagissez à cet article

Source : *L'évolution De La Carte SIM – Kaspersky Daily – | Nous Utilisons Les Mots Pour Sauver Le Monde | Le Blog Officiel De Kaspersky Lab En Français.*

---

iPhone chiffré : une boîte israélienne à la rescousse du FBI ?

iPhone chiffré : une boîte israélienne à la rescousse du FBI ?

Lundi 21 mars, le FBI a pris tout le monde de court en annonçant avoir trouvé une solution pour accéder aux données stockées sur l'iPhone chiffré de l'un des co-auteurs de la tuerie de San Bernardino, Syed Farook.
Après avoir aboyé partout que seul Apple pouvait débloquer la situation, l'administration américaine a en effet affirmé avoir reçu l'aide d'un mystérieux « tiers », annulant ainsi une confrontation prévue le lendemain même devant une cour de Californie.
En attendant le compte-rendu de cette méthode, que la justice attend d'ici le 5 avril, la presse spécialisée spécule sur l'identité de l'auxiliaire-mystère. Et avance un nom : Cellebrite.

Maître du « digital forensics »

Pour Yedioth Ahronoth (en hébreu), qui cite des sources anonymes, cela ne fait même aucun doute : c'est bien cette boîte israélienne qui a aidé le FBI.
Vidéo promotionnelle d'une solution de Cellebrite, permettant de débloquer un iPhone
Si les deux intéressés se sont refusés à tout commentaire, les spécialistes de l'informatique et du renseignement estiment l'information probable.
Il faut dire que cette firme, établie depuis 1999, est l'une des rares à maîtriser l'art du « digital forensic » dans la téléphonie mobile et le GPS.
Soit la dissection des appareils numériques, dans le cadre notamment d'enquêtes.
Le chercheur David Billard, sollicité en tant qu'expert dans des affaires de ce genre et rattaché à la cour d'appel de Chambéry, détaille :
« Le digital forensic consiste à récupérer les preuves, ou éléments de preuve, dans des appareils numériques. […]
Par exemple, extraire des vidéos d'un ordinateur dans le cadre d'une enquête sur un viol, retrouver des SMS effacés d'un téléphone portable dans le but de confirmer, ou infirmer, une complicité, etc… »

Analyse des appareils brûlés, écrasés, chiffrés…

*Or en la matière, l'inventaire de Cellebrite est fourni. **Promet de venir à bout** de matériel protégé par un mot de passe, « écrasé, cassé, brûlé ou endommagé par l'eau ». Et, plus intéressant en l'espèce :*
« d'analyser des formats d'application de données et des méthodes de chiffrement complexe et inconnu. »
*Le FBI semble d'ailleurs parfaitement conscient de ces compétences puisque l'agence a noué de nombreux contrats avec Cellebrite, relève le journaliste américain **John Paczkowski**, qui est allé fouiller dans les bases de données publiques de l'administration. A chaque fois, il est question d'acquisition de matériel de télécommunication, sans fil, relatif à l'informatique, par le ministère de la justice américain (le DOJ).*

*L'accord conclu entre Cellebrite et le FBI, le 21 mars 2016 – **DPSD / gouvernement américaine***
*En tout, 2 millions de dollars auraient ainsi été dépensés depuis 2012, **écrit Motherboard**. Qui relève un autre détail intéressant : **le 21 mars 2016**, soit le jour de l'annonce-surprise du FBI, un accord de 15 000 dollars a justement été signé avec Cellebrite.*

Cellebrite déjà sollicité… sans succès

Avant même que le journal israélien pointe explicitement vers Cellebrite, son nom revenait de toute façon déjà dans les articles sur la saga opposant le FBI à Apple.
*L'expert des appareils d'Apple Jonathan Zdziarski **prévenait déjà en septembre 2014** : malgré les précautions louables de la marque, les derniers systèmes d'exploitation de l'iPhone ne sont pas totalement inviolables. Et Cellebrite faisait selon lui parti des rares entreprises capables de fournir des solutions commerciales pour accéder aux données du téléphone.*
*Il ne pouvait être plus proche de la vérité : dans une déclaration remise à la cour appelée à trancher le contentieux entre Apple et le FBI, un ingénieur de l'agence explique avoir déjà eu recours aux services de cette entreprise ! Sans succès… jusque là, **rapporte le New York Times** ce jeudi.*

Nombreux faits d'armes

*Par le passé aussi, Cellebrite s'est démarqué par quelques faits d'armes évocateurs. Début 2016, c'était pour **avoir aidé la police néerlandaise** à lire les messages chiffrés et supprimés d'un Blackberry.*
*Huit ans auparavant, l'association américaine en défense des libertés civiles, l'ACLU, **se lançait dans une procédure** contre la police du Michigan, accusée d'utiliser illégalement les outils de Cellebrite pour fouiller dans les téléphones des suspects.*
*Au nom du Freedom of Information Act (le FOIA), l'organisation **a demandé la publication** de compte-rendus sur l'utilisation de cette solution technique. La police a rétorqué que cette publication lui coûtait des centaines de milliers de dollars et, à notre connaissance, l'ACLU n'a toujours rien reçu… [Lire la suite]*

Réagissez à cet article

Source : *iPhone chiffré : une boîte israélienne à la rescousse du FBI ? – Rue89 – L'Obs*

L'iPhone du tueur débloqué par le FBI. Fin des poursuites contre Apple

L'iPhone du tueur débloqué par le FBI. Fin des poursuites contre Apple

---

Les autorités américaines affirment avoir « accédé avec succès aux données contenues dans l'iPhone de Syed Farook » et ont demandé à la justice d'annuler l'injonction obligeant la firme à la pomme à assister les enquêteurs.

Ce déblocage a été rendu possible par *« l'assistance récente d'un tiers »* (ndlr Cellebrite), selon un communiqué de la procureure fédérale du centre de la Californie, Eileen Decker. Elle indique en conséquence avoir demandé à la justice d'annuler l'injonction obligeant Apple à aider les enquêteurs. La firme refusait de se plier aux demandes judiciaires, soutenant qu'aider à décrypter le téléphone de Syed Farook créerait un précédent, sur lequel les autorités risquaient de s'appuyer à l'avenir pour réclamer l'accès aux données personnelles de nombreux citoyens pour diverses raisons.

« Viabilité »

Lundi 21 mars, les autorités fédérales avaient annoncé être sur la piste d'une méthode qui pourrait leur permettre d'accéder aux données du téléphone. Une audience clé, qui devait avoir lieu mardi au tribunal de Riverside en Californie, avait été annulée, après le dépôt d'une motion demandant un délai pour tester *« la viabilité »* de cette solution alternative.

Le gouvernement expliquait avoir *« poursuivi ses efforts pour accéder à l'iPhone »* pendant la procédure judiciaire et annonçait que des *« tierces parties »* lui avaient présenté une manière de décrypter son contenu sans la coopération d'Apple. La police fédérale demandait un peu de temps pour s'assurer que la méthode ne *« détruit pas les données du téléphone ».*

Une semaine plus tard, il semble donc que la méthode fonctionne. Washington affirme à la cour fédérale avoir *« accédé avec succès aux données contenues dans l'iPhone de Syed Farook »* et *« ne plus avoir besoin de l'assistance d'Apple »*… [Lire la suite]

Réagissez à cet article

Source : *San Bernardino : Washington a débloqué l'iPhone du*

tueur et renonce à poursuivre Apple

Des chercheurs trouvent une faille dans le chiffrement d’Apple

	Des chercheurs trouvent une faille dans le chiffrement d’Apple

---

Des chercheurs de l'université Johns Hopkins révèlent une faille dans le chiffrement de l'application iMessage. Celle-là pourrait permettre à des pirates d'accéder aux photos et vidéos envoyées.

Issu du *Washington Post*, l'article aurait été retiré juste après sa publication ce matin, selon certains blogueurs qui réussissent néanmoins à retrouver sur Google des bribes de l'article. De nouveau visible sur le site du journal, la nouvelle pourrait faire grand bruit. Car ce matin des universitaires américains prétendent avoir décelé une faille dans le chiffrement d'iMessage, l'application de messagerie instantanée d'Apple.

La compagnie vante justement sa capacité de chiffrement « de bout en bout », qui chiffre le message au moment même de son envoi, et garantit normalement qu'aucun tiers (y compris Apple) ne puisse obtenir la clé de déchiffrement du message. Pourtant le chercheur Matthew D. Green qui a dirigé l'équipe universitaire affirme qu'une faille permettrait d'intercepter les images et vidéos. « *Cela n'aurait en rien aidé le FBI à débloquer l'iPhone du tueur de San Bernardino* », affirme-t-il, « *mais cela démontre que la notion selon laquelle ce type d'application serait infaillible est erronée.* »

Selon Green, il était insensé de demander à une société comme Apple de créer des versions modifiées de leurs produits, puisque des failles peuvent d'ores et déjà être trouvées : « *Même Apple, qui compte dans ses rangs les meilleurs cryptographes du monde, ne sont pas en mesure de créer un chiffrement 100% fiable. C'est bien ce qui me rend inquiet quand j'entends qu'en plus on parle de créer des failles volontaires dans leurs produits alors que nous ne sommes déjà pas capables de créer des sécurités imparables.* »

Le professeur Matthew D. Green, de l'université Johns Hopkins

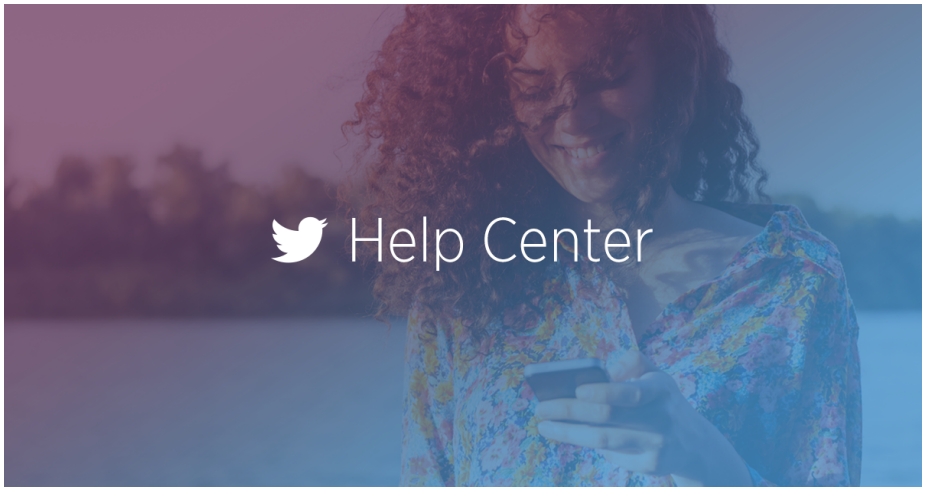
Pour intercepter le fichier, les étudiants auraient conçu un logiciel qui imite les serveurs d'Apple. La communication qu'ils ont attaquée par la suite contenait selon eux un lien vers une photo stockée sur l'iCloud d'Apple, ainsi que sa clé de déchiffrement de 64 bits.

Matthew D. Green et son équipe ont fait savoir qu'ils publieront les détails de leur attaque dès qu'Apple aura trouvé un remède à la faille découverte. Ils affirment aussi que des attaques similaires sont régulièrement pratiquées par les services de renseignement américains… [Lire la suite]

Réagissez à cet article

Source : *Des chercheurs trouvent une faille dans le chiffrement d'Apple*

Retrouvez l'historique de vos tweets depuis le tout premier envoyé



Retrouvez l'historique de vos tweets depuis le tout premier envoyé

Télécharger votre archive Twitter vous permet de parcourir les éléments publiés sur Twitter depuis votre tout premier Tweet.

Pour télécharger et visualiser votre archive Twitter :
Accédez à vos paramètres de compte en cliquant sur l’icône Profil en haut à droite de la page et en sélectionnant Paramètres dans le menu déroulant.
Cliquez sur Demander votre archive.
Une fois votre téléchargement prêt, nous enverrons un email contenant un lien de téléchargement à l’adresse confirmée associée à votre compte Twitter.
Quand vous recevez cet email, cliquez sur le bouton Télécharger maintenant pour vous connecter à votre compte Twitter et télécharger le fichier .zip de votre archive Twitter.
Dézippez le fichier et cliquez sur index.html pour voir l’archive dans le navigateur de votre choix.
Remarque : Il nous faudra peut-être plusieurs jours pour préparer le téléchargement de votre archive Twitter.
… [Lire la suite]

Réagissez à cet article

Source : *Télécharger votre archive Twitter | Centre d’assistance Twitter*

Le FBI pense pouvoir déchiffrer l’iPhone d’un terroriste sans l’aide d’Apple

Le FBI pense pouvoir déchiffrer l’iPhone d’un terroriste sans l’aide d’Apple

Alors qu'Apple refuse depuis des semaines d'aider le FBI à décrypter l'iPhone de l'un des auteurs de la tuerie de San Bernardino, le FBI vient d'annoncer qu'il tenait peut-être la solution.

La fin d'un bras de fer?

Le gouvernement américain pourrait ne plus avoir besoin des services d'Apple pour récupérer les données de l'iPhone de l'un des terroristes de l'attaque de San Bernardino survenue le 2 décembre 2015. Il a annoncé ce lundi être sur la piste d'une solution alternative. Si elle s'avère efficace, cela mettrait fin à la bataille juridique engagée depuis des semaines avec la marque à la pomme.
Une audience clé qui devait avoir lieu mardi a finalement été levée sur la demande des autorités fédérales. Les enquêteurs vont ainsi pouvoir tester « la viabilité » de leur « méthode ». Ils se sont engagés à remettre à la juge Sheri Pym d'ici le 5 avril, un rapport d'évaluation.

Les autorités optimistes

Dans un communiqué, le ministre de la justice a indiqué qu'il avait poursuivi ses efforts pour accéder à l'iPhone sans l'aide d'Apple depuis de le début de la procédure engagée contre la firme de Cupertino. Les recherches ont abouti dimanche avec la « présentation de la part de tierces parties d'une méthode possible pour débloquer le téléphone », indique le communiqué. Le gouvernement veut s'assurer que sa solution « ne détruit pas les données du téléphone », mais reste « raisonnablement optimiste ».
Les enquêteurs et les familles des victimes réclament de pouvoir accéder aux données du téléphone, potentiellement cruciales pour déterminer comment a été organisé l'attentat et si les deux terroristes ont bénéficié d'aide extérieure.

Apple de son côté campe sur ses positions

Permettre d'accéder aux données du téléphone de Syed Farook créerait un dangereux précédent qui pourrait justifier que les autorités demandent à l'avenir l'accès aux données personnelles de nombreux citoyens pour diverses raisons.
A l'occasion de la keynote d'Apple qui s'est tenue lundi, Tim Cook a justifié la position de la marque. « Nous devons décider en tant que nation quel pouvoir devrait avoir le gouvernement sur nos données et notre vie privée », a-t-il déclaré. « Nous pensons fermement que nous avons l'obligation d'aider à la protection de vos données et votre vie privée », a-t-il ajouté.
Pour rappel, le 2 décembre 2015, Syed Farook et sa femme Tashfeen Malik ont ouvert le feu dans un centre social à San Bernardino, dans l'Etat de Californie. 14 personnes ont été tuées dans la fusillade … [Lire la suite]

Réagissez à cet article

Source : *Le FBI pense pouvoir déchiffrer l'iPhone d'un terroriste sans l'aide d'Apple – L'Express*

Piratage du capteur d'empreinte d'un téléphone avec une simple imprimante à jet d'encre

Piratage du capteur d'empreinte d'un téléphone avec une simple imprimante à jet d'encre

---

Les capteurs de biométrie sont sur le grill après une nouvelle tentative fructueuse de piratage sur des téléphones Samsung Galaxy S6 et Huawei Honor 7. L'iPhone 5s a pour sa part résisté.

La biométrie serait pour beaucoup l'avenir de la sécurité, surtout en situation de mobilité. Et bien ce sont les chercheurs de l'université du Michigan qui viennent de prouver qu'une imprimante à jet d'encre pouvait à elle seule permettre de pirater les systèmes de capture d'empreinte de téléphones Samsung et Huawei. Objectif : rentrer dans le téléphone. Une imprimante à jet d'encre basique certes, mais pour réaliser ce hack, ils ont toutefois du s'équiper d'encre et de papier spécifique.
Démonstration en vidéo du hack de capteur biométrique réalisé par l'université du Michigan. (Source : Université du Michigan)

En moins de 15 minutes, selon les chercheurs qui publient une vidéo à ce sujet, il est donc possible d'entrer par effraction dans un smartphone, à condition bien sûr de récupérer l'empreinte digitale du possesseur du téléphone. Ensuite, une impression en haute résolution sur un papier brillant et une encre spécifique permet de duper le module d'analyse d'empreinte des téléphones Samsung Galaxy S6 et Huawei Honor 7. Les chercheurs précisent par ailleurs que la tentative de hack sur un iPhone 5s s'est soldée par un échec.

Pas une première, mais très peu cher et facile a réaliser

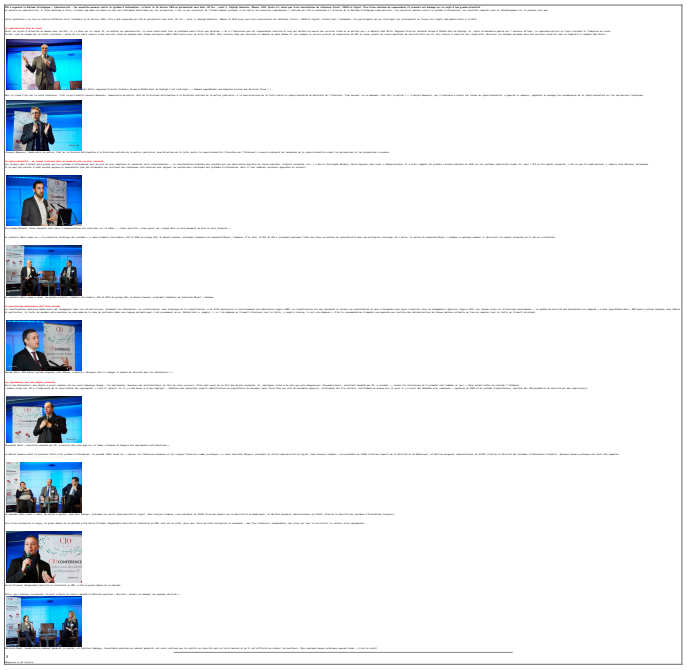
Ce n'est pas la première fois que les capteurs d'empreinte digitale sont floués par des tentatives de piratage. Mais jusqu'alors les techniques utilisées reposaient sur de l'impression 3D et des moules spécifiques. Cette nouvelle méthode s'avère de fait bien moins onéreuse, et bien plus rapide. De quoi poser quelques questions quand on sait que Samsung (et d'autres) prévoient de proposer de l'authentification de paiement avec de la biométrie.
Il convient de noter toutefois que l'utilisation de la biométrie à tord et à travers fait l'objet de critiques depuis fort longtemps. Il s'agit de ne pas confondre authentification et identification d'une part, et surtout de ne pas l'utiliser pour de l'authentification forte… [Lire la suite]

Réagissez à cet article

Source : *Capteur d'empreinte : un piratage avec une simple imprimante à jet d'encre – ZDNet*

Comment contrer les nouvelles menaces en Cybersecurité contre le système d’information ?

Comment contrer les nouvelles menaces en Cybersecurité contre le système d’information ?



Source : *Cybersécurité : contrer les nouvelles menaces contre le système d'information*

Les accessoires connectés sont en plein boom

Les accessoires connectés sont en plein boom

En plein essor, le marché des accessoires connectés a enregistré des chiffres records lors de l'année 2015.
Vous avez sûrement dû remarquer de plus en plus de personnes munies de montres ou de bracelets connectés… Peut-être en avez-vous une vous-même. Parfois critiqués pour leur esthétique peu flatteuse, les bracelets et montres high-tech ont quand même connu un gros succès l'année précédente, comme le suggèrent les chiffres publiés par l'International Data Corporation (IDC) (http://www.idc.com/getdoc.jsp?containerId=prUS41037416).

En 2015, le marché des wearables a explosé. Plus de 78 millions d'accessoires ont été vendus, soit une augmentation de 171 % par rapport à l'an passé. « L'augmentation des ventes d'accessoires connectés signifie que le marché n'est pas uniquement destiné aux technophiles. Ces accessoires sont très bien accueillis par le grand public », fait remarquer Ramon Llamas, analyste à l'IDC.

LE PALMARÈS
Mais alors quel constructeur est le grand gagnant ?
Fitbit a terminé l'année 2015 de la même façon qu'il l'a commencée, en pôle position avec plus de 21 millions de bracelets connectés vendus, soit une augmentation de 93 % par rapport aux ventes effectuées l'année précédente. Fitbit est suivi par le chinois Xiaomi à l'origine du petit bracelet connectée low cost Mi Band.

Le constructeur chinois a vendu 12 millions d'objets, ce qui représente plus de 15 % du marché. Xiaomi est suivi de près par Apple qui occupe la troisième place du podium. La marque à la pomme a vendu plus de 11 millions d'Apple Watch, ce qui représente 14,9 % de parts dans le marché des accessoires connectés et jusqu'à 50 % pour le seul marché des montres connectées. Suivent ensuite Samsung et Garmin plus loin dans le classement.

Apple, qui est devancé par d'autres fabricants dans le classement général, est toutefois le grand gagnant de l'année passée. Même si l'entreprise de Tim Cook se trouve être troisième du classement, les prix de vente ne sont pas les mêmes d'une société à l'autre. Apple a vendu onze millions d'Apple Watch à 400 euros l'unité. Alors que Xiaomi, qui a écoulé 12 millions de bracelets connectés Mi Band, le vend à 15 dollars l'unité,… [Lire la suite]

Réagissez à cet article

Source : *Les accessoires connectés sont en plein boom – Tech – Numerama*

Stocker des données pendant des milliards d’années est désormais possible

Stocker des données pendant des milliards d’années est désormais possible

---

Des chercheurs de l'université de Southampton ont annoncé avoir créé une technologie permettant « d'enregistrer des données en cinq dimensions et de les stocker pendant des milliards d'années ».

Les données sont sauvegardées sous forme de « nanostructures » gravées sur un disque de verre à l'aide d'un laser ultrarapide, dit « laser femtoseconde ». Le procédé permet d'encoder des informations en cinq dimensions: les trois coordonnées spatiales, la taille et l'orientation des nanostructures. Ces dernières modifient le trajet de la lumière à travers le verre et sa polarisation, ce qui permet ensuite de lire les données sauvegardées en utilisant à cet effet un microscope optique et un polariseur.

© FLICKR/ A HEALTH BLOG

Les pensées humaines dévoilées en temps réel par un ordinateur

Le support, dit « disque 5D », est capable de stocker jusqu'à 360 téraoctets d'information et ce, à des températures allant jusqu'à 1.000°C. Selon les inventeurs de cette technologie, il peut également rester opérationnel pendant 13,8 milliards d'années à une température ambiante.

Les scientifiques de Southampton avaient déjà présenté leur innovation en 2013, mais ils n'avaient à l'époque réussi à enregistrer qu'un fichier texte de 300 kilooctets. Depuis, ce mode de stockage a considérablement évolué, ce qui a permis d'enregistrer en 5D la Déclaration universelle des droits de l'homme, l'Optique de Newton, la Magna Carta et la Bible.

« Il est fascinant de penser que nous avons créé une technologie permettant de sauvegarder et de stocker des documents et des informations pour les générations futures. Grâce à cette technologie nous pouvons être sûrs que notre civilisation, tout ce que nous avons appris ne sera pas oublié », a déclaré le professeur Peter Kazansky, du Centre de recherche en optoélectronique (ORC) de Southampton… [Lire la suite]

Réagissez à cet article

Source : *Stocker des données pendant des milliards d'années*

est désormais possible