Les objets connectés de santé

Les objets connectés surveillant notre santé et permettant aux médecins d'intervenir avant même que le mal ne se déclare semblent l'avenir de la médecine, pourtant ils posent d'importants problèmes de sécurité car, via des smartphones, ils communiquent par Internet, un espace où les hackers veillent.

Les applications médicales en vente se comptent actuellement par dizaines de milliers et vont du pur gadget aux objets réellement utiles. Pour ne pas disserter dans le vague, voyons quelques exemples. Le plus courant semble être les bracelets d'activité que portent les joggers. Ils analysent leurs données personnelles comme le nombre de pas effectués, le pouls, *etc*. les envoient à leur smartphone où une application en déduit un certain nombre de renseignements comme le nombre de calories brûlées. Dans cet esprit, on trouve même des fourchettes connectées pour surveiller les régimes alimentaires, ceci en relation avec des balances tout aussi connectées. De même, une brosse à dents connectée peut contrôler que son utilisateur se brosse correctement les dents et prévenir l'apparition de caries. Elle peut également envoyer vos habitudes de brossage à votre dentiste.
Tous ces objets connectés collectent des données comme la température, le rythme cardiaque et toutes sortes de résultats d'analyses. Que faire de toutes ces données ? Quel est leur statut ? Tout d'abord, quelle est leur pertinence alors que, pour l'instant, il n'existe ni label, ni contrôle de la qualité de ces mesures ? Un médecin ne pourra tout simplement pas en tenir compte et sera contraint de vérifier les mesures par des analyses classiques. Pour qu'il puisse le faire, il faudrait que certaines normes soient respectées. Pour l'instant, ce n'est pas le cas même si la Commission Nationale de l'Informatique et des Libertés (CNIL) s'est penchée sur la question en 2014 dans son *Cahier Innovation & Prospective* numéro 2 : *Le corps, nouvel objet connecté*.

Suivi des maladies chroniques

Les exemples rencontrés jusqu'ici, même s'ils posent quelques problèmes éthiques, n'ont pas un intérêt vital direct. Il en est autrement pour les malades chroniques comme les diabétiques, les asthmatiques ou les insuffisants cardiaques. Dans le premier cas, une pompe à insuline connectée simplifie la vie des patients. Plus précisément, un ensemble relié à un smartphone prend en charge les injections d'insuline, le suivi de l'activité physique, la mesure de la glycémie, l'envoi et le partage des données dans le cloud. Le patient n'a plus à se soucier de rien. On retrouve les mêmes solutions pour les malades atteints d'insuffisance cardiaque nécessitant un pacemaker. Les avantages des objets connectés sont donc indéniables, quand les objets fonctionnent comme ils sont censés le faire.

Les algorithmes utilisés

Les algorithmes utilisés se localisent dans l'objet lui-même, dans son relais individuel, smartphone, tablette ou ordinateur, ou encore chez le fournisseur de services ou autres. Dans les deux premiers cas, ce sont des algorithmes usuels liés directement à l'utilisateur. Par exemple, un thermomètre connecté peut être associé à un algorithme simple permettant à une femme désirant un enfant de prévoir sa période de fertilité. D'autres algorithmes du même type, utilisant plusieurs données distinctes peuvent signaler des anomalies, qui peuvent mener à consulter un médecin. Même s'il existe un risque de provoquer l'hypocondrie, ces traitements algorithmiques locaux ne posent pas de problèmes déontologiques profonds. Il en est autrement du traitement des données collectées au niveau du fournisseur, ce que l'on nomme habituellement le *big data*. Bien sûr, il peut permettre de prévoir la naissance d'une épidémie par exemple si on repère une élévation de la température corporelle moyenne à un endroit donné. Il peut aussi permettre à certains annonceurs d'envoyer des publicités ciblées. On imagine par exemple un jogger muni d'un bracelet connecté recevoir des publicités pour des boissons énergisantes.

Les dangers des objets connectés

Au-delà de ces questions, les objets connectés posent des problèmes de sécurité multiples. Pas besoin d'entrer dans la technique pour le comprendre, il suffit de réaliser à quoi sont connectés ces objets : à Internet, directement, à travers un smartphone ou un ordinateur. Ces outils pouvant être piratés, les objets connectés peuvent l'être également, et plutôt plus facilement que les ordinateurs puisqu'ils sont à l'heure actuelle très peu protégés. Par exemple, ils ne sont en général pas munis d'antivirus et leurs capacités de chiffrement sont très limitées et difficiles à augmenter, ne serait-ce que pour des raisons de dissipation de l'énergie. Peut-on admettre des brosses à dents, des lunettes ou des verres de contact qui chaufferaient ? (voir l'encadré : les difficultés du chiffrement, page suivante).

Serons-nous un jour tous connectés ?

Les objets connectés sont donc des cibles faciles pour les pirates, pour se constituer des réseaux de zombies, ou botnets, c'est-à-dire d'ordinateurs dont ils se sont rendus maîtres pour lancer des actions malveillantes, telles l'envois de spams, des opérations de phishing, des attaques en déni de service ou des recherches exhaustives de mots de passe. Cela peut sembler de la science-fiction, comment penser que votre brosse à dents ou votre tensiomètre puisse vous envoyer des spams ? Pourtant, cela s'est déjà produit ! Selon *Proofpoint*, une société californienne de sécurité, la première cyberattaque d'envergure (750 000 spams) utilisant des objets connectés a été réalisée fin 2013. Le nombre d'objets connectés devant passer les 20 milliards en 2020 selon toutes les prévisions, le marché est immense… pour les pirates.

Dans le même esprit, l'endroit le moins défendu étant toujours le meilleur pour prendre une citadelle, on peut imaginer un objet connecté être l'objet d'attaques pour pénétrer le réseau informatique d'un hôpital, par exemple. Si les objets connectés peuvent être des outils, ainsi que des têtes de pont, pour les pirates, les données qu'ils contiennent peuvent également être attaquées, soit tout simplement volées, soit modifiées. Votre vie la plus intime peut ainsi être exposée, des appareils importants pour votre santé devenir des dangers, *etc*. Le pilulier connecté pourrait ainsi, par exemple, envoyer de fausses indications à votre médecin, de même pour le tensiomètre. L'imagination des pirates étant sans limite, ils trouveraient bien un moyen de rançonner les hôpitaux, les médecins ou les malades en menaçant de détraquer des instruments nécessaires à leur santé comme les pacemakers ou les pompes à insuline. Sans vouloir noircir le tableau à l'excès, puisque les objets connectés sont un progrès possible, il est nécessaire de comprendre qu'ils comportent aussi un problème de sécurité important, trop peu pris en compte à l'heure actuelle.

Hervé Lehning

Les difficultés du chiffrement

De nos jours, les chiffrements de qualité, c'est-à-dire difficiles à décrypter, reposent sur deux types de chiffres, utilisés en particulier dans le système *Pretty Good Privacy* (PGP). L'essentiel est un chiffrement symétrique, fonctionnant dans les deux sens (chiffrement et déchiffrment) avec la même clef. Ces chiffrements ont la rapidité de l'addition, le plus simple d'entre eux est d'ailleurs l'addition du message (qui est une liste de bits, c'est-à-dire de 0 et de 1) avec une clef aléatoire (qui est aussi une liste de bits). Dans la pratique, ils chiffrent par blocs de 128 bits comme l'AES. Le point délicat est la transmission de la clef car elle doit être changée très souvent par souci de sécurité. Celle-ci se fait via un chiffrement asymétrique tel le fameux RSA. Ce chiffrement a la lenteur d'exponentiation, opération bien plus gourmande que l'addition à effectuer. Dans un petit objet connecté au contact du corps, ou dans le corps, cette opération génèrerait de la chaleur ce qui la rend inadaptée. Sauf avancée importante en matière cryptologique, les objets connectés resteront donc des objets faciles à pirater.

Voir *l'univers des codes secrets de l'Antiquité à Internet*, Ixelles 2012