# Lorsque le code peut tuer ou guérir

La technologie a fait faire à la santé d'extraordinaires progrès. Mais libre ou propriétaire ? Dans le domaine des appareils médicaux pilotés par des logiciels ce choix peut avoir de très lourdes conséquences.

Ici plus qu'ailleurs, sacrifier l'humain sur l'autel du business model ne peut plus être une solution durable dans le temps[1].

## Lorsque le code peut tuer ou guérir

**When code can kill or cure**

*Technology Quarterly – 2 juin 2012 – The Economist*
*(Traduction : balsamic, moala, Isammoc, Otourly, Mnyo, HgO, elquan)*

**Appliquer le modèle open source à la conception d'appareils médicaux permet d'accroitre la sécurité et stimule l'innovation.**

Les pompes SMART délivrent des médicaments parfaitements dosés pour chaque patient. Des défibrilateurs faciles à utiliser peuvent ramener des victimes d'attaque cardiaque d'entre les morts. Les pacemakers et coeurs artificiels maintiennent les gens en vie en s'assurant que la circulation sanguine se déroule sans problème. Les appareils médicaux sont une merveille du monde moderne.

Alors que ces appareils sont devenus de plus en plus efficients, ils deviennent cependant de plus en plus complexes. Plus de la moitié des appareils médicaux vendus aux Etats-Unis (le plus grand marché de la santé) s'appuient sur du logiciel, et souvent en grande quantité. Ainsi le logiciel dans un pacemaker peut nécessiter plus de 80.000 lignes de code, une pompe à perfusion 170.000 lignes et un scanner à IRM (Imagerie à Résonance Magnétique) plus de 7 millions de lignes.

Cette dépendance grandissante vis à vis du logiciel cause des problèmes bien connus de tous ceux qui ont déjà utilisé un ordinateur : bugs, plantages, et vulnérabilités face aux attaques. Les chercheurs de l'université de Patras en Grèce ont découvert qu'un appareil médical sur trois vendu aux États-Unis entre 1995 et 2005 a été rappelé pour défaillance du logiciel. Kevin Fu, professeur d'informatique à l'université du Massachusetts, estime que ce phénomène a affecté plus de 1,5 millions d'appareils individuels depuis 2002. En avril, les chercheurs de la firme de sécurité informatique McAfee ont annoncé avoir découvert un moyen pour détourner une pompe à insuline installée dans le corps d'un patient en injectant l'équivalent de 45 jours de traitement d'un seul coup. Enfin, en 2008, Dr Fu et ses collègues ont publié un article détaillant la reprogrammation à distance d'un défibrillateur implanté.

Or le disfonctionnement du logiciel d'un appareil médical a des conséquences beaucoup plus désastreuses que d'avoir seulement à faire redémarrer votre ordinateur. Durant les années 1980, un bug dans le logiciel des machines de radiothérapie Therac-25 a provoqué une overdose de radiations administrées à plusieurs patients, en tuant au moins cinq. L'Organisation américaine de l'alimentation et des médicaments, l'America's Food and Drug Administration (FDA), s'est penchée sur le cas des pompes à perfusion qui ont causé près de 20.000 blessures graves et plus de 700 morts entre 2005 et 2009. Les erreurs

logicielles étaient le problème le plus fréquemment cité. Si, par exemple, le programme buggé interprète plusieurs fois le même appui sur une touche, il peut administrer une surdose.

En plus des dysfonctionnements accidentels, les appareils médicaux sans fils ou connectés sont également vulnérables aux attaques de hackers malveillants. Dans le document de 2008 du Dr Fu et de ses collègues, il est prouvé qu'un défibrillateur automatique sous-cutané peut être reprogrammé à distance, bloquer une thérapie en cours, ou bien délivrer des chocs non attendus. Le Dr Fu explique que lors des phases de test de leur logiciel, les fabricants d'appareils manquent de culture de la sécurité, culture que l'on peut trouver dans d'autres industries à haut risque, telle que l'aéronautique. Insup Lee, professeur d'Informatique à l'Université de Pennsylvanie, confirme : « Beaucoup de fabricants n'ont pas l'expertise ou la volonté d'utiliser les mises à jour ou les nouveaux outils offerts par l'informatique ».

Personne ne peut évaluer avec certitude l'étendue réelle des dégâts. Les logiciels utilisés dans la majorité des appareils médicaux sont propriétaires et fermés. Cela empêche les firmes rivales de copier le code d'une autre entreprise, ou simplement de vérifier des infractions à la propriété intellectuelle. Mais cela rend aussi la tâche plus ardue pour les experts en sécurité. La FDA, qui a le pouvoir de demander à voir le code source de chaque appareil qu'elle autorise sur le marché, ne le vérifie pas systématiquement, laissant aux constructeurs la liberté de valider leurs propres logiciels. Il y a deux ans, la FDA offrait gratuitement un logiciel « d'analyse statique » aux constructeurs de pompes à perfusion, dans l'espoir de réduire le nombre de morts et de blessés. Mais aucun constructeur n'a encore accepté l'offre de la FDA.

## Ouvert à l'étude

Frustrés par le manque de coopération de la part des fabricants, certains chercheurs veulent maintenant rebooter l'industrie des appareils médicaux en utilisant les techniques et modèles open source. Dans les systèmes libres, le code source est librement partagé et peut être visionné et modifié par quiconque souhaitant savoir comment il fonctionne pour éventuellement en proposer une version améliorée. En exposant la conception à plusieurs mains et à plusieurs paires de yeux, la théorie veut que cela conduise à des produits plus sûrs. Ce qui semble bien être le cas pour les logiciels bureautiques, où les bugs et les failles de

sécurité dans les applications open source sont bien souvent corrigés beaucoup plus rapidement que dans les programmes commerciaux propriétaires.

Le projet d'une pompe à perfusion générique et ouverte (Generic Infusion Pump), un effort conjoint de l'Université de Pennsylvanie et de la FDA, reconsidère ces appareils à problèmes depuis la base. Les chercheurs commencent non pas par construire l'appareil ou écrire du code, mais par imaginer tout ce qui peut potentiellement mal fonctionner dans une pompe à perfusion. Les fabricants sont appelés à participer, et ils sont plusieurs à le faire, notamment vTitan, une start-up basée aux Etats-Unis et en Inde « Pour un nouveau fabricant, c'est un bon départ » dit Peri Kasthuri, l'un de ses co-fondateurs. En travaillant ensemble sur une plateforme open source, les fabricants peuvent construire des produits plus sûrs pour tout le monde, tout en gardant la possibilité d'ajouter des fonctionnalités pour se différencier de leur concurrents.

Des modèles mathématiques de designs de pompes à perfusion (existantes ou originales) ont été testés vis à vis des dangers possibles, et les plus performantes ont été utilisées pour générer du code, qui a été installé dans une pompe à perfusion de seconde main achetée en ligne pour 20$. « Mon rêve, dit Dave Arnez, un chercheur participant à ce projet, est qu'un hôpital puisse finalement imprimer une pompe à perfusion utilisant une machine à prototypage rapide, qu'il y télécharge le logiciel open source et que l'appareil fonctionne en quelques heures ».

L'initiative Open Source Medical Device de l'université Wisconsin-Madison est d'ambition comparable. Deux physiciens médicaux *(NdT: appelés radiophysiciens ou physiciens d'hôpital)*, Rock Mackie et Surendra Prajapati, conçoivent ainsi une machine combinant la radiothérapie avec la tomographie haute résolution par ordinateur, et la tomographie par émission de positron. Le but est de fournir, à faible coût, tout le nécessaire pour construire l'appareil à partir de zéro, en incluant les spécifications matérielles, le code source, les instructions d'assemblages, les pièces suggérées — et même des recommandations sur les lieux d'achat et les prix indicatifs. La machine devrait coûter environ le quart d'un scanner commercial, la rendant attractive pour les pays en voie de développement, déclare le Dr Prajapati. « Les appareils existants sont coûteux, autant à l'achat qu'à la maintenance » rappelle-t-il, là ou les modèles libres sont plus durables. « Si vous pouvez le construire vous-même, vous pouvez le réparer vous-même. »

Les appareils open source sont littéralement à la pointe de la science médicale. Un robot chirurgien open source nommé Raven, conçu à l'Université de Washington à Seattle fournit une plateforme d'expérimentation abordable aux chercheurs du monde entier en proposant de nouvelles techniques et technologies pour la chirurgie robotique.

Tous ces systèmes open source travaillent sur des problématiques diverses et variées de la médecine, mais ils ont tous un point commun : ils sont encore tous interdit à l'utilisation sur des patients humains vivants. En effet, pour être utilisés dans des centres cliniques, les appareils open source doivent suivre les mêmes longues et coûteuses procédures d'approbation de la FDA que n'importe quel autre appareil médical. Les réglementations de la FDA n'imposent pas encore que les logiciels soient analysés contre les bugs, mais elles insistent sur le présence d'une documentation rigoureuse détaillant leur développement. Ce n'est pas toujours en adéquation avec la nature collaborative et souvent informelle du développement open source.

Le coût élevé de la certification a forcé quelques projets open source à but non lucratif à modifier leur business model. « Dans les années 90, nous développions un excellent système de planning des traitements de radiothérapie et avions essayé de le donner aux autres cliniques, explique le Dr Mackie, mais lorsque la FDA nous a suggéré de faire approuver notre logiciel, l'hôpital n'a pas voulu nous financer. » Il a fondé une société dérivée uniquement pour obtenir l'approbation de la FDA. Cela a pris quatre ans et a couté des millions de dollars. En conséquence, le logiciel a été vendu en tant qu'un traditionnel produit propriétaire fermé.

D'autres tentent de contourner totalement le système de régulation américain. Le robot chirurgical Raven (Corbeau) est destiné à la recherche sur les animaux et les cadavres, quant au scanner de l'Open Source Medical Device, il est conçu pour supporter des animaux de la taille des rats et des lapins. « Néanmoins, déclare le Dr Mackie, rien n'empêche de reprendre le design et de lui faire passer les procédures de certification dans un autre pays. Il est tout à fait envisageable que l'appareil soit utilisé sur des humains dans d'autres parties du monde où la régulation est moins stricte, avance-t-il. Nous espérons que dans un tel cas de figure, il sera suffisamment bien conçu pour ne blesser personne. »

## Changer les règles

La FDA accepte progressivement l'ouverture. Le Programme d'interopérabilité des appareils médicaux Plug-and-Play, une initiative de 10 millions de dollars financé par le NIH (l'Institut National de la Santé) avec le support de la FDA, travaille à établir des standards ouverts pour interconnecter les appareils provenant de différents fabricants. Cela signifierait, par exemple, qu'un brassard de pression artérielle d'un certain fabricant pourrait commander à une pompe à perfusion d'un autre fabricant d'arrêter la délivrance de médicament s'il détecte que le patient souffre d'un effet indésirable.

Le framework de coordination des appareils médicaux (Medical Device Coordination Framework), en cours de développement par John Hatcliff à l'Université de l'État du Kansas, est plus intrigant encore. Il a pour but de construire une plateforme matérielle open source comprenant des éléments communs à beaucoup d'appareils médicaux, tels que les écrans, les boutons, les processeurs, les interfaces réseaux ainsi que les logiciels pour les piloter. En connectant différents capteurs ou actionneurs, ce cœur générique pourrait être transformé en des dizaines d'appareils médicaux différents, avec les fonctionnalités pertinentes programmées en tant qu'applications (ou *apps*) téléchargeables.

À terme, les appareils médicaux devraient évoluer vers des ensembles d'accessoires spécialisés (libres ou propriétaires), dont les composants primaires et les fonctionnalités de sécurité seraient gérés par une plateforme open source. La FDA travaille avec le Dr Hatcliff pour développer des processus de création et de validation des applications médicales critiques.

Dans le même temps, on tend à améliorer la sécurité globale et la fiabilité des logiciels dans les appareils médicaux. Le NIST (Institut national des États-Unis des normes et de la technologie) vient juste de recommander qu'une seule agence, probablement la FDA, soit responsable de l'approbation et de la vérification de la cyber-sécurité des appareils médicaux, et la FDA est en train de réévaluer ses capacités à gérer l'utilisation croissante de logiciels.

De tels changements ne peuvent plus attendre. « Quand un avion s'écrase, les gens le remarquent », dit le Dr Fu. « Mais quand une ou deux personnes sont blessées par un appareil médical, ou même si des centaines sont blessées dans

des régions différentes du pays, personne n’y fait attention. » Avec des appareils plus complexes, des hackers plus actifs et des patients plus curieux et impliqués, ouvrir le cœur caché de la technologie médicale prend vraiment ici tout son sens.

## Notes

[1] Crédit photo : Patrick (Creative Commons By-Nc)