Piratage des dispositifs rythmologiques implantables : est ce dangereux ?

J. TAÏEB

Dr Jérôme TAÏEB
CH Aix en Provence

Introduction

De tous temps, les humains ont commis crimes individuels et meurtres de masse en faisant preuve parfois, de créativité redoutable. Est ce que le piratage de prothèse rythmique implantable pourrait exposer nos patients aux assassins ? En d'autre terme, est ce qu'un individu ou une organisation mal intentionnée pourrait interrompre les fonctions de stimulation cardiaque chez un patient stimulodependant ou induire une arythmie létale via un dispositif rythmique implantable ? La question fait froid dans le dos mais mérite d'être posée à l'heure du développement exponentiel de la connectivité.

Aspects technologiques

Prendre le contrôle d'un dispositif rythmologique implantables (DRI) de type Pacemaker (PM) ou Défibrillateur automatique implantable (DAI), implique une connexion électronique avec accès aux options de programmation.
Il existe 3 types de communications avec une prothèse rythmique. Seule la première est disponible pour tous les boitiers.

1- Programmation en face à face direct : Apres mise en place de la tête de programmation au contact de la prothèse, le programmateur de la marque permet d'accéder à toutes les fonctions de programmation et de recueil de données. La tête de programmation doit rester au contact de la loge du boitier pendant toute la durée de la communication

2- Programmation en face à face à courte distance : La mise en place de la tête de programmation permet l'établissement de la connexion mais celle ci peut ensuite être poursuivie à une courte distance en retirant la tête de programmation. La communication est réalisée par voie hertzienne. La distance maximale est de 5 à 6 m et il existe une temporisation puisque la connexion s'interrompt automatiquement après un délai de quelques minutes sans activité.

3- Télésurveillance des prothèses à longue distance : Cette technologie permet de recueillir les informations de la prothèse par voie hertzienne depuis le domicile du patient. La communication s'établit avec un boitier transmetteur qui envoie les informations recueillies au médecin responsable via une centrale sous le contrôle du constructeur. Les envois sont réalisés de façon automatique à des horaires définis ou, manuellement par le patient. Cette transmission permet le transfert de données depuis la prothèse vers le médecin lecteur mais aucune modification des paramètres de programmation de la prothèse n'est possible à distance par cette méthode.

Alertes sécurité

Plusieurs alertes de sécurité sont parues récemment dans la presse. Nous en citerons 2 :
• En 2017, la FDA a enquêté à la suite d'informations selon lesquelles les pacemakers Abott comportaient des failles de sécurité informatique pouvant permettre à une personne non autorisée d'accéder à l'appareil. La société Abbott a répondu en créant un logiciel correctif appelé firmwire qui n'a toutefois pas été téléchargé systématiquement en raison de la survenue d'évènements indésirables rares et aléatoires à type d'asystolie. De nombreux patients ont en effet refusé cette mise à jour pour prévenir des failles de sécurité exclusivement théoriques dans la mesure ou aucun cas de piratage n'a été rapporté.
Abbott a également souligné que l'information a été communiquée en premier lieu au fond d'investissement Muddy Waters au moment de l'acquisition de Saint Jude par Abbott. Cette démarche a eu un impact sur le cours de l'action faisant suspecter un conflit d'intérêt plutôt qu'une réelle volonté de protéger les patients d'un risque de piratage.

• En mars 2019 les autorités fédérales américaines ont lancé un avertissement concernant les défibrillateurs Medtronic. Des chercheurs de la société de sécurité Clever Security ont rapporté que les données échangées via le protocole conexus entre ces appareils et programmateurs ne sont pas cryptées, qu'il n'existe aucune sécurité pour y accéder. Ils ont surtout montré qu'il est possible de prendre le contrôle des DAI pendant la fenêtre de communication ouverte lors d'une session de télésurveillance soit 0,02% du temps. Mais vouloir exploiter cette faille implique d'agir au bon moment, d'être à proximité du DAI, de connaître les références du boitier, ainsi que les codes de programmation et enfin la physiologie cardiaque !.
La société medtronic a répondu en créant un cryptage actualisé dans sa nouvelle gamme Azure.

Buzz, Fantasme et paranoia

Ces composantes de nos sociétés modernes s'invitent dans la discussion et aident à comprendre l'agitation médiatique autour du piratage informatique des DRI.
En 2007, Jonathan Reiner le cardiologue du vice président américain Dick Cheney a fait désactiver les fonctions de télésurveillance à distance sur le DAI de son patient en expliquant qu'il redoutait une programmation malveillante possible depuis une chambre d'hôtel mitoyenne. La notion de proximité apparaissait dans sa déclaration. Cette information a inspiré un épisode de la série Homeland ou l'on voit le vice président américain être assassiné par un terroriste devant son ordinateur. Il s'agit d'un cas fictif qui semble parfaitement impossible puisque la prothèse n'est à aucun moment reconnue par une tête de télémétrie et la manipulation se fait à longue distance avec une simple récupération du numéro de série.
En 2013, le célèbre hacker Jack Barnaby a été retrouvé mort quelques jours avant de participer à la conférence Black Hat ou il devait faire une présentation sur la sécurité des dispositifs médicaux implantables sans fil. Ce timing avait donné lieu à des théories du complot d'un assassinat par le gouvernement ou par une des entreprises médicales dont les produits avaient été hackés. Par la suite, l'enquête a conclu à une overdose.

La vraie question : « Le jeu en vaut il la chandelle ? »

Le piratage informatique implique une logistique conséquente : Proximité de la cible, matériel sophistiqué pour se connecter, information sur le modèle de la prothèse, connaissances rythmologique et de programmation des DRI.
Les motivations d'une cyber attaque peuvent être politique (espionnage, modification de vote électronique, ..), économique (rançon, revente de données..), criminelle (assassinat de leader, terrorisme..).
Un patient implanté d'un PM ou DAI n'est pas une cible motivante pour des hackers malveillants. Et si pour une quelconque raison, un projet de meurtre concernait un patient porteur de DRI, il existe des méthodes bien plus éprouvées que le piratage électronique. Ajoutons, que la programmation d'un DRI laisse des traces informatiques et que les constructeurs améliorent leurs protections comme tous les fabricants de matériels informatiques et de logiciels de protection.
Si un assassinat individuel ou de masse était programmé, le hacking de PM ou DAI est probablement une des méthodes les moins engageantes.

Conclusion

Il est possible d'entrer en communication avec une prothèse rythmique, même si aucun cas de piratage malveillant de DRI n'a été décrit.
La complexité technique et la nécessité d'une proximité immédiate de la prothèse rend cette méthode de malveillance heureusement non attractive.
Dans une société qui recherche le buzz et la sécurité absolue, il faut s'attendre à de nouveaux titres à sensation et à de nouvelles alertes sécurités ainsi qu'à un renforcement continu des protections informatiques des DRI.

Bibliographie

- Muddy Waters Capital LLC. MW is short St. Jude Medical (STJ:US). Muddy Waters Research.2016. https://d.muddywatersresearch.com/research/stj/mw-is-short-stj/. Accessed February 13, 2018.
- U.S. Food and Drug Administration. Cybersecurity vulnerabilities identified in St. Jude Medical's implantable cardiac devices and Merlin@home transmitter: FDA safety communication. U.S. Food and Drug Administration.2017. https://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm535843.htm. Accessed February 13, 2018.
- Baranchuk A, Refaat MM, Patton KK, Chung MK, Krishnan K, Kutyifa V, Upadhyay G, Fisher JD, Lakkireddy DR; American College of Cardiology's Electrophysiology Section Leadership. Cybersecurity for cardiac implantable electronic devices: what should you know?J Am Coll Cardiol. 2018; 71:1284–1288. doi: 10.1016/j.jacc.2018.01.023
- FDA Alert mars 2019 : https://www.reuters.com/article/us-medtronic-cyber/fda-says-cybersecurity-vulnerabilities-found-in-some-medtronic-devices-idUSKCN1R300H
- Kramer DB, Fu K. Cybersecurity concerns and medical devices: lessons from a pacemaker advisory. JAMA. 2017; 318:2077–2078. doi: 10.1001/jama.2017.15692