

PACEMAKERS & ICD: CYBERSICUREZZA E HACKERAGGIO

Il punto di vista di un vecchio tecnico marketing

Quando nel settembre del 1967 scendevo in bicicletta da Ingegneria (porta Saragozza) ed entravo dal cancello sui viali al Policlinico S.Orsola, per fare gli ECG in Semeiotica Chirurgica diretta dal Prof. Leonardo Possati, non immaginavo di certo che prima o poi mi sarei dovuto occupare di pacemakers. Né tantomeno che i pacemakers sarebbero stati tutta la mia vita professionale. Ora come socio APDIC con grande piacere scrivo questo mio punto di vista, ovvio da pensionato del settore, in merito ai vari rumors ed articoli sull'hackeraggio di pacemakers ed ICD.

1. Premessa

Ho assistito come tecnico al primo impianto di pacemaker in Sala Operatoria del S.Orsola nel 1967. Di seguito ed in estrema sintesi o di corsa ricordo a tutti che i primi pacemakers erano solo stimolatori quindi una batteria e un interruttore elettronico che per 70 volte al minuto collegava la batteria ai fili (elettrodi) posizionati nel cuore. La filosofia era di salvare la vita a tutti quei pazienti che erano riusciti a sopravvivere alla crisi di MAS ed avevano una frequenza spontanea di 20 battiti al minuto. La tecnologia costruttiva e la filosofia era: tutto ciò che non c'è non si può rompere, quindi non pone problemi.

Come più volte ci hanno illustrato il Prof Boriani ed il Dr Biffi, ricercatori e scienziati hanno lavorato e continuano a lavorare per il costante miglioramento dei dispositivi impiantabili da almeno 70 anni. Riassumendo queste sette decadi si può dire:

- *decade anni 40*: primo pacemaker artificiale esterno creato da John Hopps nel 1949;
- *anni 50*: Earl Bakken nel 1957 realizza il primo pacemaker esterno “portatile”;
- *anni 60*: Rune Elmqvist crea tre modelli di pacemaker Elema E135, E137, E142 con differenti batterie il 135 con nichel-cadmio gli altri due con batterie zinco-mercurio, sempre nella decade anni 60 vennero creati altri modelli da Zoll nel 1961 e da Kantrowitz nel 1962, simili agli Elema ma più attenti alla estetica del prodotto;
- la decade degli *anni 70* è importante perché introduce l'innovazione delle batterie al litio, il contenitore o cassa in titanio, le batterie con radioisotopo al Plutonio-238; ma, soprattutto, la telemetria a radio frequenza e verso la fine della decade i primi pacemaker doppia camera;
- *decade anni 80*: i primi defibrillatori (ICD) impiantabili, i pacemakers Rate-Response dotati di sensore (ad esempio movimento, respiro, QT, ecc.);
- *decade anni 90*: gli anni 90 sono una decade....tranquilla. Elemento importante la introduzione dei *microprocessori* come circuito elettronico capaci di gestire la stimolazione ed i vari sensori e di *memorizzare* molte informazioni;
- *decade anni 2000*: due importanti progressi in questa decade e precisamente la stimolazione *biventricolare*, prima nei pacemakers poi negli ICD, ma particolarmente importante la seconda novità: il **controllo in remoto**, ovvero la trasmissione dal device impiantato, via Telefono/Internet, ad un centro raccolta dati, realizzando così il controllo medico senza contatto fisico tra paziente e medico;
- *decade anni 2010*: come possibile alternativa agli *elettrodi di stimolazione* vengono sviluppati pacemakers *wireless* utilizzando gli ultrasuoni per stimolare un ricevitore senza fili nel cuore. Un'altra soluzione prevede un ricevitore, senza fili nel cuore, che utilizza campi magnetici al posto degli ultrasuoni.

Lo sviluppo, oggi, è quindi dedicato a rendere i device impiantabili più accessibili o *user-friendly* e protetti.

2. Pacemakers Cyber-Attacks

I pacemakers ed ICD di oggi sono equipaggiati con un *microprocessore integrato* per permettere la gestione di tutte le funzioni che comportano milioni di combinazioni tra le varie aree, stimolazione, sensing, sensori, terapie, memorie, ecc.

Il microprocessore inserito nel device deve poter dialogare con un *computer* esterno o programmatore o interfaccia remota tramite una *backdoor*. Come ogni altro dispositivo elettronico remoto la *backdoor* non è immune da attacchi cyber e da essere utilizzata per penetrare nel device, ovviamente per buone o cattive intenzioni. Esistono protezioni *crittografiche* che permettono al pacemaker di respingere certi segnali ed autorizzare l'accesso solo a quelli consentiti. Già nel 2015 Barnaby Jack, direttore della sicurezza dei dispositivi con microprocessore integrato, per la società di sicurezza I O Active , ha studiato la possibilità di cyber-attacchi a dispositivi medici ed ha realizzato un primo dispositivo in grado di penetrare dispositivi *wireless* impiantati quali pompe da insulina ed alcuni pacemaker .Il dispositivo realizzato è stato costruito sulla base di un processo di reverse-ingegnerizzazione che ha rilevato diversi difetti in molti dispositivi biomedicali.

Personalmente credo che l'enorme sviluppo e produzione di *manichini/simulatori/oggetti dimostrativi* realizzati da tanti diversi produttori ed adottati dalle aziende leader di Pacemaker ed ICD con tanto anzi tantissimo *wireless*, spesso usando circuiti o parti di dispositivi o programmatori clinici, abbia creato una vera *autostrada* per gli *hacker*.

Sempre a livello personale penso che, se vengono impiantati oggi nel mondo circa 600.000 dispositivi all'anno, che si vanno a sommare ai pazienti impiantati precedentemente, sia probabile che oggi nel mondo ci siano tre o quattro milioni di pazienti portatori di pacemaker o ICD *wire-less*.

Come diceva un vecchio politico ... "a pensare male è peccato, però spesso ci si prende". Ecco il mio pensare male è: se oggi ci sono tre o quattro milioni di pazienti con dispositivi che al proprio interno hanno memorizzati tali e tanti dati personali, medici statistici, clinici, allora conviene provare ad hackerarli per ottenere una *banca dati* mondiale da vendere a produttori di mille cose specifiche per pazienti con quelle caratteristiche o pensare a nuovi mercati.

Quindi gli attacchi *hacker* sono pubblicizzati come rischio di morte per i pazienti. Sono, a mio avviso, una degenerazione delle leggi di mercato, si pensi, a titolo esemplificativo, al tentativo di costringere le aziende produttrici a comperare sistemi anti -hacker dalle stesse società che finanziano gli hacker.

3. Soluzioni

Non sono un esperto informatico, anzi mi lamento sempre con mio figlio ingegnere perché il mio pc a volte prende strane iniziative, però da anziano vedo che nell'*informatica* in generale esistono da tempo almeno tre tipi di protezione:

- *Jammer* - Viene normalmente inserito in tutti i dispositivi di scansione ad esempio i sistemi radar.
- *Firewall* - Ovvero *Muro di Protezione*. Per impedire l'ingresso agli Hacker si alza un muro (o crittografia del dispositivo). È la soluzione più focalizzata sul software e viene largamente utilizzata in tutti i dispositivi con accesso ad internet.
- *Password Look o Blocco Password*. Una terza soluzione per il controllo e la prevenzione di attacchi informatici sarebbe una password bloccata e specifica per ogni singolo dispositivo impiantabile. Tuttavia il problema principale con questo tipo di sicurezza è che la password dovrebbe essere conosciuta solo dal paziente. Molti pacemaker di oggi hanno già una loro password specifica secretata e conosciuta solo dai programmatori dedicati.

Pare che gli ultimi attacchi Hacker a pacemaker o ICD siano stati possibili per una *fuga* di password, o lasciate erroneamente in chiaro in alcuni programmatori o comperate al mercato nero da alcuni Hacker.

4. Situazione oggi

Mi limito di seguito a riportare quello che ho letto su Internet o nei siti dedicati ai Cyber Attack delle Aziende di Devices.

16 settembre 2016: Lettera del Dr Mark Carlson – Vice President and Chief Medical Officer, ai pazienti del "Sistema Merlin" di SJM dichiara che ... il 25 Agosto 2016 Muddy Waters Capital, una agenzia internazionale di investitori, con l'obiettivo di *trarre profitto da una riduzione del prezzo delle Azioni di*

St.Jude Medical ha distribuito un rapporto relativo alla vulnerabilità in materia di Cybersicurezza nel sistema SJM Merlin@home ... I pazienti possono contattare negli USA il numero 1-877-MY-MERLIN o visitare il sito SJM o contattare il proprio medico.

1 settembre 2017 - La Food and Drug Administration (FDA), ente statunitense che si occupa della sicurezza di alimenti, farmaci e dispositivi clinici, *aveva diffuso nei giorni scorsi un avviso stimando in 465.000 negli USA i device St JUDE MEDICAL /ABBOT contenenti un difetto di sicurezza nel loro software che potrebbe essere sfruttato per causarne malfunzionamenti.* Oggi 1 settembre 2017 la ABBOT, che ha acquistato SJM, ha riferito alla BBC che ci sono altri 280.000 pacemaker con lo stesso difetto in altri paesi del mondo, senza fornire molti dettagli in più.

I pacemaker coinvolti hanno un sistema di trasmissione e ricezione radio, che viene utilizzato per scaricare i dati sanitari che hanno raccolto e, se necessario, per inviare loro un aggiornamento al software. Un hacker potrebbe quindi inviare un codice malevolo via radio, a patto di essere sufficientemente vicino per effettuare la trasmissione dei dati a corto raggio. Sono comunque richieste capacità tecniche notevoli: *ABBOT dice di non avere ricevuto notizia di nessun attacco tentato o andato a buon fine.*

Sintesi

*745.000 pazienti con pacemaker con difetto di cybersicurezza nel mondo
Di questi 465.000 negli USA e 280.000 in EUROPA*

Conclusioni

I nuovi pacemaker distribuiti in questi giorni sono già aggiornati, quindi potranno essere impiantati senza particolari problemi.

ABBOT dichiara che i modelli che hanno il potenziale problema di software e che necessitano di “software update” sono solo le seguenti famiglie di prodotti con telemetria wireless RF:

Accent SR RF; Accent ST; Accent MRI; Accent ST MRI; Accent DR RF; Assurity; Assurity +; Assurity MRI; Anthem RF; Allure RF; Allure Quadra RF; Quadra Allure MP RF; Quadra Allure; Quadra Allure MP.

ABBOT nel proprio sito internazionale ha pubblicato una *Guida per pazienti* codice SJM-CRM-0817-0092a (Item approved for international use).

In estrema sintesi ABBOT, nella *Guida per pazienti*, premette che dispositivi con tecnologia software così importante è normale che possano necessitare di un aggiornamento o up grade.

ABBOT invita i pazienti portatori dei device sopra elencati a contattare il proprio Centro e verificare con il proprio Medico o Team:

- informarsi sul modello che gli è stato impiantato;
- chiedere quali siano le opzioni alla prossima visita di controllo.

Se necessaria verrà consigliata una procedura di aggiornamento non invasiva, che richiede circa 3 minuti e viene effettuata tramite un trasmettitore radio. C'è la possibilità che l'aggiornamento comporti una perdita di parte dei dati sanitari già raccolti dal dispositivo o come in un recente passato un numero molto basso di pacemakers dopo aggiornamento abbiano avuto malfunzionamenti

Ogni paziente è unico! Spetterà quindi ai medici ed ai pazienti decidere cosa fare, valutando se sia più rischioso tentare l'aggiornamento o mantenere il pacemaker con la falla, o rimandare la sua installazione in attesa di nuovi sviluppi.

Chiudo con la mia ultima opinione personale ... io sono sicuro che tutto il Team S.Orsola sia Medico che Tecnico sia in grado di gestire con tranquillità e professionalità anche questo evento.

Credo inoltre che APDIC possa/debba mettere nel proprio sito un link o pagina di CyberAttack o sollecitare AIAC a farlo a livello nazionale.

Grazie per l'attenzione

Paolo Pagani

23 ottobre 2017