Capitolo 9

PANCREAS ARTIFICIALE E RISCHI INFORMATICI DA INTEGRAZIONE CON LO SMARTPHONE

Daniele Giansanti (a), Umberto Ferrante (b), Rosario Alfio Gulino (b), Lisa Monoscalco (b), Maurizio Lucentini (a), Alessandro Spurio (a), Giovanni Maccioni (a), Mauro Grigioni (a)
(a) Centro Nazionale Tecnologie Innovative in Sanità Pubblica, Istituto Superiore di Sanità, Roma
(b) Facoltà di Ingegneria, Università di Tor Vergata, Roma

Componenti del pancreas artificiale

Il pancreas artificiale è un sistema a *loop* chiuso, che viene sviluppato per migliorare le condizioni di vita di soggetti affetti da diabete di tipo 1, riducendo così il tempo che essi impiegano nell'autocura. Questo dispositivo prende appunto il nome di pancreas artificiale perché non fa altro che riprodurre la funzione endocrina del pancreas attraverso le seguenti componenti:

1. sensore che misura la glicemia, ovvero il valore di glucosio nel sangue;
2. ricevitori ed elaboratori *wearable* in tempo reale;
3. pompa d'infusione d'insulina;
4. algoritmo di controllo che determina la quantità di insulina da infondere nel paziente.

La componente 3 risiede in un dispositivo portatile, generalmente uno smartphone che ha il ruolo di elaboratore e monitor, che comunica tramite *Bluetooth* con le altre componenti.

In un sistema a *loop* chiuso tutte queste componenti sono interconnesse tramite una rete wireless e appositamente testate per essere interconnesse tra di loro in un unico dispositivo medico come nel caso del recente dispositivo medico pancreas artificiale immesso in commercio negli Stati Uniti.

Cybersecurity e pancreas artificiale

In un sistema eterogeneo quale è il pancreas artificiale, la connessione wireless, che permette alle componenti di comunicare tra di loro, crea un ambiente potenzialmente suscettibile agli attacchi cibernetici (1-4). Se la connessione tra dispositivo *wearable* per il monitoraggio continuo del glucosio e il microcontrollore nello smartphone non fosse sicura potenzialmente un malintenzionato potrebbe inviare dati deliberatamente errati all'algoritmo di controllo il quale potrebbe determinare il rilascio di un'elevata quantità di insulina determinando una situazione di ipoglicemia nel paziente; il corpo risponderebbe ad una situazione di ipoglicemia attraverso il rilascio di glucagone ed epinefrina e perdurando la situazione verrebbero compromesse le funzionalità cerebrali, motorie e cognitive, fino anche a causare la morte. Pensando ai componenti del pancreas artificiale e tanto per fare un esempio, si pensi che in commercio sono presenti sia pompe d'insulina, dotate di cifratura e oscuramento dei dati pertanto protette dal tampering che pompe di insulina che usano una semplice rete aperta. Venendo alla tipologia di attacchi come è ben noto gli attacchi che sfruttano la connessione wireless possono essere passivi, quali l'*eavesdropping*, ovvero l'origliamento delle comunicazioni per collezionare dati da usare poi in modo non appropriato, oppure attivi, che consistono nel prendere il comando del *device*, determinando situazioni di pericolo per il paziente.

Un attacco cibernetico che sfrutta una vulnerabilità wireless è un attacco esterno, ci possono essere anche attacchi interni che possono compromettere l'integrità del software. Questi ultimi attacchi possono sfruttare *malware* (*virus, spyware, trojan*), che molto spesso possono trovarsi negli elaboratori mobili o fissi connessi al dispositivo-sistema. Anche questi tipi di attacchi possono o collezionare e divulgare informazioni confidenziali o prendere il controllo del *device.* Molti sistemi eterogenei di pancreas artificiali sperimentali, come evidenziato in uno studio di O'Keeffe *et al*. (1), integrano dispositivi che non sono stati valutati per funzionare in tali configurazioni, e quando vengono utilizzati in questo modo, la comunità che si occupa di ricerca clinica dovrebbe essere consapevole dei problemi potenziali per la sicurezza. Per tenere conto di queste problematiche la Food and Drug Administration ha messo a disposizione linee guida e raccomandazioni che si sono susseguite negli anni nei relativi archivi pubblici online.

Considerazioni finali

In questo studio si sono volute evidenziare delle potenziali problematiche inerenti alla cybersecurity, alla connessione wireless di diverse componenti biomedicali, per creare il cosiddetto pancreas artificiale. Studi in questo ambito si stanno sviluppando nel territorio nazionale. Tali studi coinvolgono anche l'Istituto Superiore di Sanità che è impegnato su diversi fronti che vanno dalla regolamentazione, allo sviluppo di metodiche di test e valutazione, alla terza missione che nel caso specifico ha riguardato attività di ricerca attraverso tesi in collaborazione tra il Centro Nazionale Tecnologie Innovative in Sanità Pubblica e la Facoltà di Ingegneria dell'Università di Tor Vergata in Roma anche dedicate alla stima del danno economico da attacco, un aspetto particolarmente rilevante che implica lo sviluppo di modelli economici specifici dedicati e complessi per via della eterogeneità del danno. È evidente inoltre come il pancreas artificiale è solo uno dei tanti dispositivi impiantabili attivi che presenta potenziali problematiche di cybersecurity. Oggi praticamente tutti i dispositivi impiantabili attivi presentano un'opportunità di manutenzione e riprogrammazione remota tramite connessione wireless come ad esempio i pacemaker, i neurostimolatori cerebrali, gli stimolatori gastrici, gli impianti cocleari. Questa connessione, mette da un lato a disposizione una *backdoor*, dall'altro apre al rischio da potenziali cyberintrusioni, come ad esempio evidenziato nei pacemaker (5). Una illustrazione di queste problematiche esula tuttavia dall'obiettivo di questo studio meritando di essere affrontata in una trattazione ampia e specifica.

Bibliografia

1. O'Keeffe DT, Maraka S, Basu A, Keith-Hynes P, Kudva YC. Cybersecurity in artificial pancreas experiments. *Diabetes Technol Ther* 2015;17(9):664-6.
2. Doyle FJ, Huyett LM, Bok Lee J, Zisser HC, Dassau E. Closed-loop artificial pancreas systems: engineering the algorithms. *Diabetes Care* 2014; 37:1191–1197.
3. Picton PE, Yeung M, Hamming N, Desborough L, Dassau E, Cafazzo JA. Advancement of the artificial pancreas through the development of interoperability standards. *J Diabetes Sci Technol* 2013;7:1066-70.
4. Maisel WH, Kohno T. Improving the security and privacy of implantable medical devices. *N Engl J Med* 2010;362:1164-6.
5. Baranchuk A, Alexander B, Campbell D, Haseeb S, Redfearn D, Simpson C, Glover B. Pacemaker cybersecurity. *Circulation* 2018;138(12):1272-3.