

## قرصنة الأجهزة الطبية الملتصقة والمزروعة بالمرضى

د. محمد سعيد غزال (\*)

### الملخص

رغم ما قدمته الشبكات من فوائد عظيمة في إيصال المعلومات أو التطبيقات المحوسبة لمحتاجيها، فهي أيضاً سهلت عمليات الاختراق لهذه المعلومات والتطبيقات وغيرها من المصادر الحاسوبية. ويفسر هذا كون الشبكات وسيطاً جيداً لنقل الخبيث من البيانات والبرامج كما هي للطبيب منها. وحيث إننا لا نستطيع الاستغناء عن الشبكات في حياتنا اليومية أفراداً وشركات وحكومات، كان التحدي المستمر هو في ضرورة مقايضة Tradeoff بعض المميزات مثل السرعة والمستوى العالي من الأداء في مقابل الحصول على أمان أكثر. وساعد توافر الشبكات اللاسلكية (وهي أقل حماية من نظيرتها السلكية) والتطبيقات الكثيرة والمتجددة على أجهزة الهاتف الذكية وخاصة في تطبيقات إنترنت الأشياء Internet of things أو IoT والتي تستخدم الشبكات اللاسلكية كوسيط أساسي للنقل في توسع المشكلة وزيادة تعقيدها. وتوجد تقنية إنترنت الأشياء حالياً في الكثير من التطبيقات المنزلية والمركبات الحديثة، وحتى في تطبيقات الأجهزة الطبية الملتصقة بجسد المريض أو المزروعة داخل جسده (WIMDs) Wearable and Implantable Medical Devices) والمستخدم في تنظيم علاج الأمراض المزمنة كمرض السكري والسرطان ومرض القلب وغيرها. والبحث عبارة عن دراسة مسحية Survey Study في أدبيات موضوع قرصنة الأجهزة الطبية (المحوسبة) الملتصقة أو المزروعة، وتحديدًا جهازاً ناظم نبض القلب Implantable Cardiac Defibrillator (ICD)، ومنظومة ضخ الأنسولين (أو ما يسميه البعض بالبنكرياس الصناعي) والمكونة من مضخة أنسولين وجهاز تحكم. ويوضح البحث إمكانية اختراق هذه الأجهزة وبالتالي انتهاك خصوصية المريض بالإضافة لإمكانية التعديل على برمجياتها ومن ثم التحكم فيها عن بعد بواسطة أجهزة بسيطة ومتوافرة بسعر مقبول مثل الريموت كونترول و راديو البرمجيات Software Radio. كما يشرح البحث المخاطر المحتملة من هكذا اختراق، والحلول المناسبة (الفنية والإدارية) لمنع (أو تقليل) هذه المخاطر.

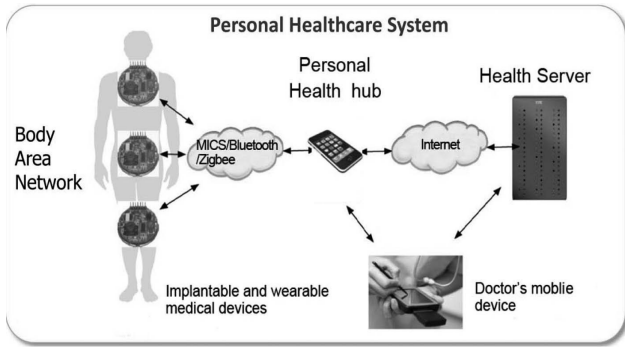
### المقدمة

كثيرة لاستخدام تكنولوجيا إنترنت الأشياء في تسهيل أو حتى تمكين الحياة لقطاعات كبيرة ومتزايدة من ذوي الاحتياجات الخاصة والمرضى بأمراض مزمنة مثل السكري وارتفاع ضغط الدم وغيرهم.

ومن التطبيقات الطبية المحوسبة الأجهزة الطبية المزروعة (IMD) Implanted medical devices) أو الملتصقة بجسد المريض من الخارج (WMD) Wearable medical devices)، وكلا النوعين (يسميان اختصاراً WIMDs) يهدف لتوفير الدواء أو العلاج بشكل مستمر للمرضى المصابين بأمراض مزمنة مثل السكري، أمراض القلب، السرطان، الصمم، الأمراض العقلية والعصبية، وغيرها من الأمراض (الشكل (١)). أشهر مثال على الأجهزة الطبية المزروعة داخل الجسد ناظمت نبض القلب

أصبحت الإنترنت جزءاً أساسياً من حياة الكثير من البشر في العمل والترفيه والتعلم وغيرها من النشاطات. فمن استخدام البريد الإلكتروني كوسيلة لتداول الوثائق الرسمية أو السحابة الرقمية لتخزين البيانات والبرامج المستخدمة في مكان العمل، إلى تطبيقات محوسبة في المنزل والسيارة والسوق وغيرها. والبيت الإلكتروني مثلاً والذي يعتمد تكنولوجيا إنترنت الأشياء (وهي تطبيقات حاسوبية مدمجة داخل الأجهزة المنزلية) صار حقيقة موجودة على أرض الواقع لها مستخدموها الكثير من العجزة والمسنين الذين لا يستطيعون الاعتماد على أنفسهم في القيام بأعمال اعتيادية مثل إغلاق الأبواب وإطفاء المصابيح ليلاً [١]. وقس على ذلك أمثلة أخرى

(\*) عضو الهيئة العلمية بكلية أمن الحاسب والمعلومات، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.



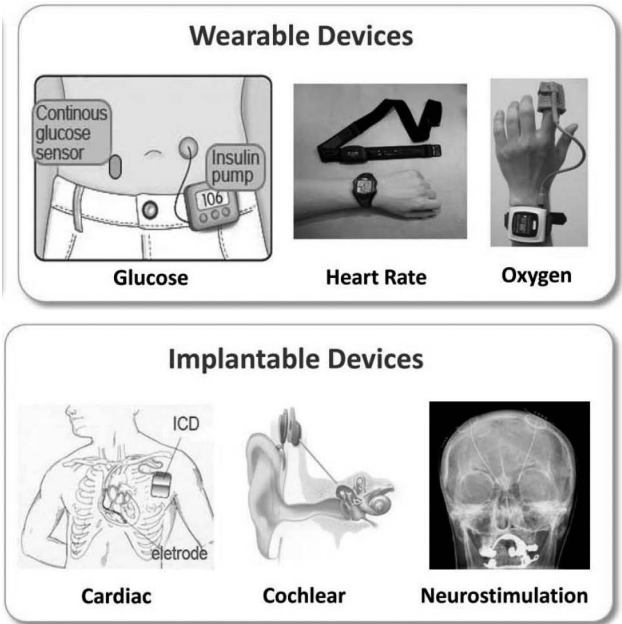
الشكل (٢): النظام الصحي الشخصي PHS . نقلا عن

[٢].

والأجهزة الطبية المزروعة أو المصققة ليست بجديدة، ولا حتى التطبيقات الحاسوبية في هذه الأجهزة هي جديدة. ما هو جديد هو استخدام الشبكات اللاسلكية لنقل البيانات الحيوية أو ما يسمى بالقياسات عن بعد Telemetry، التي ترسلها الأجهزة إلى أجزاء أخرى من الشبكة الصحية الشخصية وينتهي بها الأمر في خادم متخصص للتطبيقات الصحية والذي يقوم بدوره بالتواصل مع الطبيب أو شركة التأمين ما يسهل معرفة حال المريض ومدى نجاعة العلاج المعطى له والتدخل في حالة الطوارئ (عند فشل الجهاز في أداء مهمته مثلاً) بالتحكم أحياناً في عمل هذه الأجهزة عن بعد أو جلب المريض بشكل فوري للمستشفى. وأعطى هذا التواصل عن بعد ميزة عظيمة وهي تمكين المريض من الحياة بشكل مشابه للشخص الطبيعي من حرية التنقل والذهاب للعمل وغيرها من النشاطات دون الحاجة لزيارة الطبيب بشكل متكرر أو البقاء في المستشفى لفترات طويلة [٣].

ومن أهم نقاط ضعف التطبيقات الحاسوبية هي افتقارها لوسائل قوية وضامنة لأمن البيانات والبرامج المستخدمة فيها في مواجهة الاختراق الذي يؤدي لسرقة البيانات أو التخريب أو كليهما. ويعزى هذا الضعف لعدة عوامل منها الفني (أخطاء برمجية مثلاً)، أو عامل الخطأ البشري لأسباب نفسية أو جسدية (فسيولوجية). من ناحية أخرى، ويعزو البعض هذا الضعف أيضاً لسرعة تطور تكنولوجيا المعلومات وتطبيقاتها. فقد تطورت هذه التكنولوجيا بسرعة أكبر بكثير من نظيراتها السابقة (تكنولوجيا المواصلات مثلاً)، ما حرم تكنولوجيا المعلومات الوقت الكافي للتجربة ووضع وسائل الأمان والحماية لها. ومما فاقم المشكلة استخدام الشبكات وخاصة

الآلية Pacemakers أو نظيرتها المحوسبة Implantable Cardiac Defibrillators (ICD). أما أشهر الأجهزة خارج الجسد فهي منظومة ضخ الأنسولين والمكونة من مضخة أنسولين Insulin Pump والتي توفر الأنسولين لجسد مريض السكري حسب أوامر جهاز التحكم (الجزء الثاني من المنظومة) والذي يقوم بقياس مستوى السكر في الدم<sup>(١)</sup> قبل تحديد حاجة الجسم من الأنسولين وتوقيتها.



الشكل (١): بعض التطبيقات المحوسبة في الأجهزة الطبية المزروعة أو المصققة. نقلا عن [٢]

وتشمل الأجهزة الخارجية أيضاً ما يسمى بشبكة سطح الجسد Body Area Network (BANs)، والتي تعمل عمل المجسات التي توضع على جسد المريض في المستشفى لقياس مؤشرات الجسد الحيوية (درجة الحرارة وضغط الدم .. إلخ)، كما تعمل كشبكة إلكترونية تستخدم الجسد البشري كوسيط ناقل يربط جميع الأجهزة الطبية المستخدمة من قبل شخص واحد أو ما يسمى بالنظام (المعلوماتي) الصحي الشخصي Personal Health System (PHS)، كما يظهر في الشكل (٢). وتتحكم في هذه الأجهزة برمجيات حاسوبية تحدد كمية الدواء (أو العلاج) التي يحتاجها المريض في لحظة ما بناءً على البيانات الحيوية المدخلة لجزء التحكم في الجهاز المزروع.

(١) مجموع هذه الأجهزة يسمى البنكرياس الصناعي عند البعض رغم أنه مصطلح غير شائع بين المختصين.

أجزاء تشمل المقدمة في الجزء الأول، أهداف البحث وأهميته في الجزء الثاني، وملخص الأبحاث والدراسات ذات الصلة في الجزء الثالث، وأخيراً الخاتمة في الجزء الرابع. الجزء الثالث وهو الجزء الأساسي في البحث وينقسم بدوره لثلاثة أجزاء: الجزء ٣ - ١ وفيه نعطي صورة مختصرة ولكن شافية للجهازين الطبيين مدار البحث، والجزء ٣ - ٢ وفيه مختصر لكل الأبحاث المتعلقة بقرصنة الجهازين وفيه نوضح الوسائل والنتائج لمحاولات هذه القرصنة ومدى خطورتها، والجزء الثالث وفيه نشرح الوسائل الفنية والإجرائية لمواجهة احتمال قرصنة الأجهزة الطبية الموصلة أو المزروعة وذلك حسب الأبحاث المستخدمة في الدراسة. ونود أخيراً أن نوضح أن الهدف الرئيس من البحث هو تقديم هذا الموضوع الحديث نسيباً للقارئ العربي المتخصص من خلال عرض مختصر لأدبيات الموضوع دون تحليل أو إضافة علمية مميزة.

## أهداف البحث وأهميته

### أهداف البحث

حيث إن الشبكات هي الوسيط الوحيد لتمكين الطبيب من التواصل عن بعد مع الأجهزة الطبية المزروعة أو الموصلة بجسد المريض WIMDs، فإن خطر قرصنتها بات يتعدى المعروف من المخاطر ليصبح خطراً على سلامة وربما حياة المستخدم. فتعطل جهاز ناظم نبض القلب (بسبب هجوم متعمد من خلال الشبكات مثلاً) قد يؤدي لوفاة المريض بسبب ارتفاع ضغط الدم الناتج عن ازدياد معدل نبض القلب، وقس على ذلك أيضاً مضخة البنسلين التي يؤدي تعطلها إلى جلطات دماغية بسبب ازدياد معدل سكر الدم، أو الإغماء (وربما الموت) في حالة نقص هذا المعدل عن الوضع الطبيعي.

وبالتالي يمكننا تحديد مشكلة (أهداف) البحث في النقاط التالية:

١ - توضيح طبيعة الأجهزة الطبية المحوسبة والمزروعة في جسد المرضى، وتحديدًا جهاز ناظم نبض القلب، ومنظومة ضخ الأنسولين.

٢ - تحديد طرق قرصنة هذه الأجهزة والمخاطر الممكنة من قرصنتها من خلال قياس تأثيرات المناح الأساسية الثلاث

العالمية منها (الإنترنت) لنشر البيانات والتطبيقات الحاسوبية بين أعداد هائلة من البشر بسرعة وبشكل شبه مجاني. وجاءت الشبكات اللاسلكية في تطبيقات الهواتف الذكية لتضاعف قاعدة وعدد المستخدمين للتطبيقات الحاسوبية إلى مئات وربما آلاف الأضعاف. وقد أصابت مشكلة السرعة هذه حتى الهيئات المنظمة لاستخدام وإنتاج الآلات الطبية المحوسبة (مثل الـ FDA في الولايات المتحدة مثلاً) بسبب قلة الخبرة في مجال فحص الجزء المحوسب من هذه الأجهزة والثقة الزائدة بهذه التكنولوجيا وقدراتها ما عجل في إصدار رخص لها وزاد من عدد المسترجع منها بسبب أخطاء برمجية عدة أضعاف ما كانت عليه قبل عشر سنوات مثلاً.

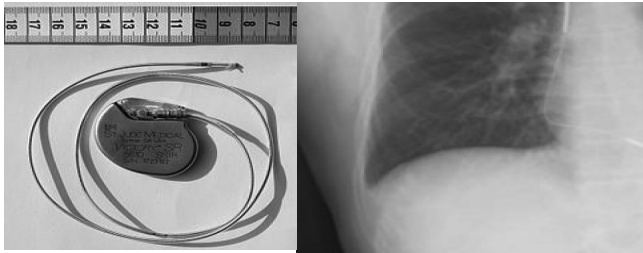
وكما يحصل في التطبيقات المحوسبة الأخرى والتي تستخدم الشبكات من قرصنة وهجمات تخريبية، فإن التطبيقات الطبية المحوسبة مثل ناظمت نبض القلب (ICDs) ونظم ضخ الأنسولين معرضة هي الأخرى لمخاطر الاختراق والقرصنة. لكن الفارق الرئيس بين النوعين من القرصنة يكمن في نتائج الاختراق والتي تتعدى عنصري التعدي على الخصوصية والخسائر<sup>٢</sup>، إلى المخاطر المحتملة على سلامة المستخدم الجسدية والنفسية واحتمال الوفاة بسبب انقطاع العلاج أو زيادته عن الحد المقبول طبيًا. وصحة الإنسان طبعًا لا تقاس بثمن ولا يمكن مقارنتها بالخسائر المالية أو السمعة التجارية أو الملاحظات القانونية لما للنفوس البشرية من قيمة مجتمعية ودينية عالية تجمع على أهميتها أغلب المجتمعات المتحضرة. هذه المخاطر الصحية تستوجب مجهودات قطاعات واسعة من المجتمع (تشمل المبرمجين والأطباء والوزارات المختصة بترخيص هذه الأجهزة مثل وزارة الصحة وحتى المرضى أنفسهم) لمواجهتها وإيجاد الحلول المناسبة لها. وهذا العمل البحثي هو جزء من هذا المجهود.

والبحث عبارة عن دراسة مسحية Survey Study في أدبيات موضوع قرصنة الأجهزة الطبية (المحوسبة) الموصلة أو المزروعة، وتحديدًا جهاز ناظم نبض القلب Implantable Cardiac Defibrillator (ICD)، ومنظومة ضخ الأنسولين (أو ما يسميه البعض بالبنكرياس الصناعي) والمكونة من مضخة أنسولين و جهاز تحكم CGS. وينقسم البحث لأربعة

(٢) خسائر مالية أو في المصادر الحاسوبية من بيانات وبرامج، أو في الأسرار التجارية، أو السمعة وغير ذلك من خسائر ناتجة عن الاختراق.

البشر والآلات ومكنت المعلومة (وهي أساس أي تطور) من الوصول لجميع من يتصل بهذه الشبكة. ومن ذلك أيضا تمكين الشبكات من توصيل كل شيء بأي شيء (إنترنت الأشياء) والذي شمل فيما يشمله أجهزة ناظم نبض القلب، أجهزة تنظيم ضخ الأنسولين، وأجهزة التحفيز العصبي الدماغي.. إلخ التي مكنت الكثيرين من العيش بشكل طبيعي وسهلت (من خلال الشبكات) تواصلهم مع الأطباء لتمكين علاجهم بشكل فوري وعن بعد.

كان لاخترع جهاز النابض في خمسينيات القرن الماضي أثر عظيم في تمكين علاج مرضى القلب، تحديدا أولئك الذين يعانون من عدم انتظام ضربات القلب، وبشكل متواصل [٣] و [٤]. حيث يعمل الجهاز على قياس النبض وتحديد نوع العلاج الفوري بناءً على هذا القياس (تخفيض معدل النبض أو زيادته مثلا). هذا الجهاز يعمل بشكل آلي وقد تطور ليصبح أصغر حجما ويستمد طاقته من بطارية طويلة العمر ما مكن الأطباء من زرعه داخل القفص الصدري للمريض (انظر الشكل ٣). وقد زرع من هذه الأجهزة ما يقارب النصف مليون جهاز خلال عام ٢٠٠٨ في الولايات المتحدة فقط، ٧٠٪ منها ICDs والباقي Pacemakers. أما على المستوى العالمي فيقدر الخبراء عدد أجهزة ال-ICD المزروعة في الفترة ما بين وحيث إن إنترنت



الشكل (٣): جهاز ناظم نبض القلب، حجمه وموضعه داخل الجسم، نقلا عن [٥].

عامي ١٩٩٧ و ٢٠٠٣ بحوالي ٤٠٠ إلى ٤٥٠ ألف جهاز [٦].

الأشياء غزت هذا النوع من الأجهزة، تمت حوسبة الناظمت وشبكها لاسلكيا بهدف تحسين أدائها وزيادة الدقة في خياراتها. تقوم البرمجيات الموجودة في الجهاز ببث إشارات تمثل البيانات الحيوية للقلب Cardiomgram Readings، عادة على شكل تقرير برسومات بيانية (تخطيط القلب) يقرؤها الطبيب المختص للتأكد من صلاحية الجهاز وللتدخل وقت الحاجة بالتحكم

لأمن المعلومات والمختزلة في الرمز (CIA) بهذه القرصنة: السرية Confidentiality، المصداقية Integrity، وتوفر خدمة الجهاز (الإتاحة) Availability. ولا نتعرض في البحث بشكل مفصل للمخاطر الصحية الناتجة عن القرصنة رغم إشارتنا لها في عدة أماكن من البحث.

٣- الحلول الفنية والإجرائية الممكنة لمنع أو تخفيف أثر الهجمات على الأجهزة محل البحث.

### أهمية البحث

تكمن أهمية البحث في أنه يسلط الضوء على موضوع الأمن الصحي وسلامة المرضى بأمراض مزمنة ممن يستخدمون الأجهزة الطبية المحوسبة لعلاجها، وتحديدًا حمايتهم من القرصنة لهذه الأجهزة وما ينتج عنها من آثار. الموضوع حديث نسبيًا، كما أن البحث فيه باللغة العربية يكاد يكون معدومًا. هذا هو من أوائل البحوث في هذا المجال باللغة العربية (إن لم يكن الأول) ما نرجو أن يشجع البعض من الباحثين العرب للتبحر في مجال أمن الأجهزة الطبية المحوسبة عموما والمزروعة/ الملصقة بجسد المريض WIMDs خصوصا علنا نتج شيئًا مفيدًا للإنسانية ونواكب ركب البحث العلمي الحاسوبي.

### قرصنة الأجهزة الطبية الملصقة أو المزروعة والحلول المناسبة لمنعها أو التخفيف من آثارها

يمكن تقسيم الدراسات السابقة في المجال إلى ثلاثة أجزاء: الجزء الأول ويعنى بتطور هذه الأجهزة وكيفية عملها حاليًا، والجزء الثاني وهو متعلق بأنواع الهجمات وأغراضها، والجزء الثالث والأخير يوضح طرق منع قرصنتها أو التخفيف من آثار هذه القرصنة.

### ١ - الأجهزة الطبية المزروعة أو الملصقة: حالتنا ناظم

#### نبض القلب و البنكرياس الصناعي

تميز القرن الماضي بالتطور الهائل في مجال الصناعة بمختلف أنواعها ومنها الصناعات الدوائية والعلاجية ما اتضح أثره في تحسين الحالة الصحية للإنسان بشكل كبير. وكانت خاتمة القرن الفريد متمثلة بتطور الحاسب وتطبيقاته في جميع مناحي الحياة، وتطوير وتفعيل شبكة الإنترنت التي ربطت



## ٢- قرصنة الأجهزة الطبية: الطرق والآثار

قبل الخوض في شأن قرصنة الأجهزة الطبية المزروعة من نوع ICD و البنكرياس الصناعي، يجب النظر وبشكل مختصر لتاريخ الأجهزة الطبية المحوسبة ومدى أمانها. فالإحصائيات تدل على أن أكبر سبب لحوادث الوفاة والإصابات الخطيرة من جراء استخدام الأجهزة الطبية المحوسبة هي الأجهزة نفسها أو البرمجيات المستخدمة في التحكم في عمل هذه الأجهزة. كما نلاحظ أيضاً أن مثل هذه الأخطاء قديمة الوجود قدم تقنية الحاسب نفسها. وكما أوضحنا في المقدمة، فإن أخطاء النظم الحاسوبية كثيرة ومتكررة لأسباب عديدة لم تعط من الوقت والجهد ما يكفي لحلها ما زاد في عدد الحوادث ودرجة فداحتها مع الوقت. ولا ننسى أخيراً ذكر العامل البشري. فكثير من الأخطاء تحصل بسبب الإهمال أو عدم المعرفة من قبل الفنيين المشغلين للأجهزة الطبية، وثقة عمياء في تكنولوجيا بشرية قابلة جداً للخطأ. وأفضل مثال على ذلك هو ما حصل من جراء استخدام جهاز «ثيراك ٢٥» Therac-25 في أواسط ثمانينات القرن الماضي، وهو جهاز طبي محوسب كان يستخدم في علاج مرضى السرطان بواسطة الأشعة وبشكل آلي. فقد تسبب استخدام الجهاز في عدة مستشفيات في الولايات المتحدة بموت ستة مرضى وإصابة العديد الآخرين منهم بحروق ومشاكل صحية أخرى [١١]. وكما حصل في قضية ثيراك ٢٥ كان للأجهزة المزروعة نصيبها من حوادث الوفاة وإصابات أخرى بسبب الأعطال الفنية في الأجهزة نفسها. فمن النصف مليون مريض الذين حصلوا على جهاز ICD مزروع خلال الفترة ١٩٩٧-٢٠٠٣ تم تسجيل ٢١٢ حالة وفاة بسبب فشل خمسة أنواع من هذه الأجهزة حسب سجلات إدارة الغذاء والدواء الفدرالية FDA في الولايات المتحدة [٦]. وأحد هذه السجلات يشير إلى حدوث ماس كهربائي في الجهاز [١٠] أدى لوفاة شاب في عمر ٢٢ سنة.

وفي ما يخص قرصنة الأجهزة الطبية المزروعة، بدأ الأمر للكثيرين أول الأمر وكأنه جزء من مسلسل Homeland حين قرصن قاتل ماجور ناظم نبض القلب pacemaker الموجود في صدر نائب الرئيس الأمريكي ما تسبب في تعطيله ومن ثم تسبب في قتله [١٢]. لكن بالنسبة للباحثين، وتحديدًا في عام ٢٠٠٦ وما تلاه، كان الأمر احتمالاً يمكن الحدوث

في عمل الجهاز عن بعد، ما أتاح للمريض الكثير من الحرية في التنقل والعمل وزاد من كفاءة الطبيب والعملية العلاجية ككل [٧]. ورغبة في تقليل تدخل الطبيب إلى أدنى حد، أضيف مؤخراً جهاز خارجي يسمى المبرمج (وهو جهاز تحكم قريب جداً من جهاز ال-ICD) يلتقط إشارات النابض ويقوم بدور الطبيب المشروح آنفاً لكن بشكل آلي. ولتمكين الطبيب من مراقبة ما يحصل مع المريض طورت آليات كثيرة لنقل البيانات (عن طريق هاتف ذكي مثلاً) من «المبرمج» إلى خادم تطبيقات يعمل كوسيط بين المرضى المشتركين في الخدمة وأطبائهم. لم يصمم ال-ICD لاستقبال الإشارات البعيدة (أكثر من ١٠ سنتيمترات) كنوع من الحماية للجهاز وبالتالي فهو يعتمد على نفسه في عمله وعلى التدخلات القليلة من «المبرمج». كما أنه صمم ليعيش داخل الجسد طول عمر المريض. لكن الهجمات الناجحة على أجهزة ال-ICD تعتبر خطيرة جداً كون إصلاح الجهاز أو استبداله يستلزم عملية جراحية لإخراجه من جسد المريض [٦] و [٨].

وبنفس النسق والأهداف تم تطوير نظام ضخ الأنسولين للتعامل مع مرضى السكري والذين يعانون عادة من فشل البنكرياس في إنتاج وضخ الكمية المناسبة من الأنسولين لمعادلة مستوى السكر الطبيعي في الجسم. النظام مكون من مضخة أنسولين وجهاز تحكم منفصل يوجه المضخة بتحديد الكمية المناسبة وتوقيت ضخ الأنسولين لجسد المريض. يقوم جهاز التحكم بعمله بناءً على معطيات (بيانات القياسات الحيوية لجسد المرضى) ويسمى عادة مراقب الجلوكوز (Glucose Monitor). قد يتصل المراقب مباشرة بالمضخة وقد يتواصل معها من خلال شبكة محيط الجسد BAN، انظر الشكلين ١ و ٢ السابقين. تعمل المضخة لمدة قصيرة لا تزيد على الأسبوع إلا أن ذلك أفضل بكثير من طرق الحقن التقليدية والتي تجبر المريض في الحالات الشديدة من المرض على حقن نفسه ٤ إلى ٧ مرات يومياً [٩]. كما أن وجود المضخة وجهاز القياسات الحيوية خارج الجسد يسهل تغييرها أو التحول عنها للعلاج التقليدي في حالة تعطلها لأسباب آلية أو بسبب هجوم القرصنة على برمجياتها. وقدرت أعداد هذه الأجهزة في الولايات المتحدة فقط سنة ٢٠٠٥ بربع مليون جهاز، وتوقع الخبراء زيادة مضطردة في عدد هذه الأجهزة حول العالم لتجاوز عدة ملايين حالياً [١٠].

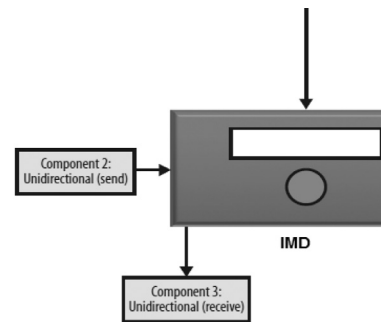
التجارية ضعيفة الحماية والمعتمدة على الشبكات اللاسلكية، وتحديدًا أحد أجهزة نابض القلب ICD المتوافرة سنة ٢٠٠٨. إدعائنا بريادة بحث فو مبني على الحقائق التالية: فهو أول من قام بدراسة عملية لإمكانية قرصنة جهاز ICD كما أن أغلب البحوث من بعده في المجال اتبعت نفس النهج و جرت حلوله وطورت عليها. أثبت فو إمكانية قرصنة جهاز ال-ICD وتخريبه بوسائل بسيطة ورخيصة نسبيًا. فباستخدام تقنية الهندسة العكسية Reverse Engineering استطاع الباحثون معرفة الثغرات والمنافذ التي يمكن من خلالها القيام بالهجمات لاحقًا، ثم قام (من خلال جهاز راديو برمجيات Software Radio متوفر وبسعر بسيط) ببيت إشارات الراديو للقيام بهجمات خطيرة مثل التجسس (Eavesdropping) على الإشارات المرسله للمبرمج وهجمات الإعادة (Replay Attacks) والتي شملت الكثير من التعديلات على بيانات المريض وطريقة العلاج أو عمل تسارع في نبض المريض. كما أثبت إمكانية القيام بهجمات منع الخدمة DoS وذلك بإغراق الجهاز بطلبات خدمة تستنفذ طاقة البطارية مما يعطلها وبالتالي يعطل الجهاز عن العمل مما يعرض حياة المريض للخطر. الملاحظة الرئيسية في شأن الهجمات أنها كلها تمت من خلال مسافة قصيرة جدا من الجهاز (من واحد إلى بضعة سنتيمترات) وهو يجعل الهجمات محدودة لكن ممكنة جدا في غرف المستشفيات التي تعج بالناس ومنهم القراصنة بالطبع.

ولم يكن فو Fu أول من فكر في تأثير هجمات منع الخدمة DoS على بطاريات الأجهزة الصغيرة مثل ال-ICD. ففي بحثه سنة ٢٠٠٤ قام مارتين [١٤] Martin بتفريغ شحنات بطارية هاتف نقال بواسطة هذا النوع من الهجمات. وكذلك الأمر في الهجمات من خلال مسافات قريبة باستخدام موجات الراديو: فبحث هاسلستاينر [١٥] Haselsteiner شرح كيفية القيام بذلك، في حين وضع هايز Hayes [١٦] مبكرًا التأثير السيئ لموجات الراديو المنبعثة من الهواتف النقالة على نوابض القلب. أما ماثور [١٧] Mathur فقد أوضح كيفية اختراق موجات اللاسلكي بسهولة من خلال ما سماه التخاطر Telepathy.

وعلى منوال فو قام راغوناثان [١٨] بقرصنة نظام أنسولين لمعالجة مرضى السكري مكون من جزء مهمته مراقبة مستوى الجلوكوز (CGS) والتحكم في ضخ الأنسولين (من مضخة

وبالتالي تجب دراسته، وخاصة بعد ورود أخبار عن حادث وفاة الشاب المذكور أعلاه بسبب تعطل بطارية الجهاز. وما شجع الباحثين فعلاً على القيام بدراساتهم هو معرفتهم اليقينية بضعف وسائل الحماية للشبكات اللاسلكية والمستخدم في أغلب النظم التجارية المتوافرة وقتها (والتي لازالت تستخدم حتى الآن). فهذه الأجهزة في معظمها إن لم يكن كلها تستخدم برمجيات حماية تعتمد وسائل أخرى غير التشفير (وهو أقوى وسيلة مجربة لحماية الشبكات اللاسلكية). برامج الحماية هذه غالبًا ما تكون برمجيات محمية بقوانين حماية الملكية الفكرية ما يجعل التعديل عليها بطريقة قانونية شبه مستحيل [٢]. كما أن معظم هذه الأجهزة قادرة على الإرسال والاستقبال (انظر الشكل ٤) ما يسهل قرصنتها بأدوات مثل جهاز التحكم عن بعد Remote controller.

وما يهمننا هنا هي المخاطر الناتجة عن قرصنة ناظم نبض القلب ونظام ضخ الأنسولين واللذان حصلنا على أكبر عدد من البحوث. وتحديدًا المخاطر الممكنة على المناحي الثلاثة المحددة لأمن المعلومات والمختزلة في الرمز (CIA): السرية (Confidentiality، ٢) المصدقية (Integrity، ٣) وتوفر الخدمة Availability. لكن الخطر الأكبر ربما يكمن في فقدان الثقة في هذه الأجهزة الطبية المحوسبة من قبل مستخدميها ما يعرض صحتهم لخطر أكبر ناتج عن «عدم» استخدام أجهزة ضرورية لحياة سوية وشبه طبيعية. هذا الخطر هو نتيجة حتمية إذا ما أفضت الأبحاث لتأكيد سهولة وإمكانية قرصنة الأجهزة الطبية المزروعة.



الشكل (٤): جهاز IMD تقليدي. المصدر [١٣].

ويعتبر كافن فو Fu [٤] (ومجموعة البحث معه بقيادة د. هالبرين حيث كان فو وقتها طالب دكتوراه) رائد البحث العلمي في مجال قرصنة الأجهزة الطبية المزروعة IMDs

عدم التحقق بعد محاولات الدخول باستخدام بيانات كاذبة. كسابقه فو و رادكليف أثبت ناكموب عملياً سهولة اختراق الأجهزة الموصولة أو المزروعة وعدم وجود أي آلية في هذه الأجهزة للدفاع ضد القرصنة والتجسس. ومن المفيد في بحث ناكموب تنبيهه لإمكانية القرصنة في العيادات الصحية والمستشفيات المزودة بخدمة واي فاي مجانية لتتيح للقرصان الدخول وبسهولة على الشبكة وتحليل البيانات الواردة فيها ومن ثم تحديد الأجهزة الضحية ومهاجمتها. ودعا في بحثه لسد هذه الثغرة بتوعية المراكز الطبية لخطورها وحثها على إيجاد وسائل أكثر أماناً ضد القرصنة والتنصت على شبكات الواي فاي المستخدمة داخلها.

طبعاً لم يجرب الباحثون أعلاه إختراقاتهم على جسد بشري بل استخدموا مواد مشابهة لأنسجة الجسد التي يزرع فيها جهاز الـ IMD. استخدم فو [٤] مثلاً لحوم الحيوانات في تجاربه. لذلك قام جليسون [٢٠] باستخدام جهاز محاكي للإنسان (مانيكين Mannequin) يستخدمه الممرضون وغيرهم من طلاب الطب والتمريض في التدريب على قياس المؤشرات الحيوية وتغيرها بسبب المرض أو الإصابات الخطيرة (انظر الشكل ٥). لم يهدف جليسون بذلك إلى استبدال مادة التجريب بقدر ما أراد التنبيه إلى خطورة الهجمات على أجهزة التدريب مثل الـ iStan في إفشال تدريب الممرضين وغيرهم وما يسببه ذلك من آثار مستقبلية مثل تخريج ممرضين وفنيين غير مؤهلين، أو انعدام الثقة بهذا النوع من الأجهزة الضرورية والمكلفة<sup>(٣)</sup> للتعليم. وقام جليسون وبمعاونة فريق من طلاب علوم الحاسب في جامعة ألاباما الجنوبية South Alabama، وباستخدام أدوات بسيطة متوافرة لأمثالهم، بمهاجمة جهاز iStan بهدف تحديد المنافذ أو الثغرات وبناءً عليه قام الطلاب بممارسة ما تعلموه من طرق الهجوم التقليدية (مثل هجمات منع الخدمة DoS، والاختراق الغاشم Brute Force Attack) ما أدى إلى تعطل الجهاز أحياناً أو قيام الجهاز بعمله ولكن بشكل خاطئ أحياناً أخرى. وتمت الإختراقات والهجمات التالية من مسافة قريبة من الجهاز ما يؤكد الفكرة أن المسافة عامل مهم جداً في تحديد نجاح الهجوم من عدمه. ورغم أن [٢٠] لم يدع أن تجارب طلابه تثبت التأثير القاتل على جسد بشري حقيقي جراء هجوم برمجي عن

(٣) تكلفة هذا النوع من الأجهزة تتجاوز المئة ألف دولار [٢١].

الأنسولين) من خلال اختراق الشبكة الرابطة لأجزاء النظام بعضها ببعض بما فيها تلك المتصلة بالمبرمج والهاتف الذكي. فباستخدام الهندسة العكسية لبروتوكولات الشبكة والتجسس عليها eavesdropping استطاع راغوناثان التحكم في مضخة الأنسولين وبتغيير بيانات المقاييس الحيوية من جهاز قياس الجلوكوز استطاع تغيير كمية العلاج وتوقيته ما أوحى بإمكانية قتل المريض من خلال القرصنة.

لكن ما قام به رادكليف [٩] سنة ٢٠١١ من قرصنة لنظام التزود بالأنسولين الخاص به كان له وقع أكبر. فرادكليف مصاب بالسكري من الدرجة الأولى (وبالتالي يهيمه الأمر شخصياً) كما أنه قام بنشر نتائج تجاربه في مؤتمر مغطى إعلامياً بشكل كبير وهو مؤتمر القبة السوداء Black Hat للقرصنة المنعقد في الولايات المتحدة سنوياً. أثبت رادكليف أن الهجوم على مجس مستوى السكر في الدم CGS كان سهلاً للغاية في حين تطلب الهجوم على المضخة معرفة الرقم التسلسلي لها وهو رقم لا يمكن إيجادها عن بعد باستخدام هجمات شبكية. وهذا اقتضى من رادكليف (أو أي مهاجم) وجوده بقرب المضخة وهو أمر صعب لكن غير مستحيل على المهاجم. وقد تمكن رادكليف من القيام بهجوم انتحال وتحايل Spoofing على جهاز الـ CGS وتغيير البيانات عن مستوى السكر في الدم. الهجوم التالي كان على المضخة نفسها حيث قام بتغيير مقاييس الضبط Configuration Settings في الجهاز بحيث تعطي كمية أكبر من الأنسولين لكل وحدة نشويات وهو ما قد يؤدي إلى الإغماء أو حتى الوفاة. وكانت المضخة التي جربها رادكليف من النوع الذي تدخل فيه البيانات يدوياً من قبل مستخدميه. وحيث إن التوجه كان نحو أتمتة عمل المضخة اعتماداً على بيانات الـ CGS، توقع رادكليف زيادة الخطورة على الجهاز لفقدان عنصر التحكم البشري في العملية [٩].

وفي وقت لاحق قام الألماني ناكموب Knackmuß [١٩] بإجراء تجارب هجوم على وحدة ضخ أنسولين. لاحظ ناكموب سهولة القيام بهذا العمل من خلال استخدام شبكات الواي فاي غير المحمية والموجودة في أغلب المستشفيات. قام الباحث بعمل عدة أنواع من هجمات القرصنة تشمل التشمم Sniffing، المسح Scanning، والاختراق الغاشم Brute Force Attack. كما اكتشف الثغرات الواضحة في خادم الويب مثل



الهيئات المنظمة مثل الـ FDA السليبي في زيادة هذه المخاطر. فالـ FDA وتحت ضغوط من المستشفيات والمستخدمين تحاول ترخيص أكبر عدد من هذه الأجهزة دون الفحص الكافي والطويل والذي تجر به عادة على الأدوية الجديدة. ومما زاد في تعقيد المشكلة هو تعاظم المستشفيات عن تسجيل حالات الخطأ في هذه الأجهزة خوفاً من الملاحقة القانونية [٢٧] من قبل المرضى أو ذويهم.

### ٣- الحلول الفنية والإجرائية لمنع قرصنة الأجهزة الطبية المزروعة أو التخفيف من آثارها

قبل سرد الحلول الفنية والإجرائية (الإدارية) من الأبحاث المغطاة في دراستنا هذه، يجب أن نذكر أن أمن المعلومات دائماً يستوجب نوعاً من التضحيات Tradeoffs. فزيادة الأمان عادة تعني قلة الفعالية والكفاءة. إنها معادلة صعبة لكن يمكن تحقيقها بناءً على معرفة تامة بمدى التضحيات التي يمكن تقديمها وقبولها من قبل المستخدم والأطراف المهم الأخرى من التشريعيين والمصنعين. ويزداد الأمر صعوبة في حالة تأمين الأجهزة الطبية المحوسبة. فالتضحيات هنا على الأغلب قليلة أو شبه معدومة. الخطر على صحة وحيات المريض أمر لا يمكن مقايضته بأي فائدة أخرى. كما أن طريقة العيش الحر التي وفرتها مثل هذه الأجهزة لا يمكن أن يتخلى عنها المستخدم طواعية. لذا كان لا بد من الاستمرار بالبحث عن حلول جديدة وخلقة (فنياً وإدارياً) لضمان الجودة العالية جداً والمثالية مع أمان عالٍ وسعر معقول للجهاز وخدماته.

ومن أوائل الباحثين في المجال كما أسلفنا من قبل هو فو [٤]. في عمله المميز سنة ٢٠٠٨ حاول فو Fu إيجاد حلول للمشاكل التي تسبب بها من خلال قرصنته لجهاز نابض قلب تجاري شائع الاستعمال. وقد نبه في بحثه إلى ضرورة إيجاد حلول جديدة ومختلفة عن الوسائل التقليدية المستخدمة في أمن الشبكات لأنها قد لا تجدي نفعاً كون الجهاز يعمل في بيئة حيوية (جسد الإنسان) ما يصعب تطبيق الوسائل التقليدية. فمثلاً طريقة تكوين مفاتيح لعملية التشفير لا تجدي نفعاً في حالات الطوارئ. ونفس الشيء يقال عن طريقة حجب أي

بعد، إلا أننا لا يمكننا إلغاء مثل هذا الاحتمال من أن يستنتج.



الشكل (٥): جهاز محاكاة الإنسان آي ستان iStan وتوابعه من CAE Healthcare [٢١] و [٢٢].

ورغم الإمكانية النظرية للاعتداء على مرضى يستخدمون أجهزة طبية مزروعة IMDs، فإن عدد الحالات المسجلة لهذا النوع من الهجمات قليل جداً [٣] و [٩]. والواقع أن أغلب الشكاوي الموجهة للمجلس الأمريكي للغذاء والدواء FDA لأجهزة طبية مزروعة لا تشمل مثل هذا النوع من المخاطر [٢٣]. وفي نهاية المطاف ما هي الأسباب التي قد تدعو أحدهم للاعتداء على مريض يحمل في جسده ناظماً لنابض القلب؟ باستثناء الشخصيات العامة والهامة من سياسيين<sup>(٤)</sup> وغيرهم، فإنه على الأغلب لا توجد أسباب منطقية للاعتداء على المواطن العادي [٢٤]. لكن التهديد بالاعتداء بهدف ابتزاز المرضى ممكن جداً في ظل وجود دلائل للممارسات شبيهة تستخدم برمجيات الفدية Ransomware، وهي برامج قرصنة يطلب المعتدي فيها من الضحية دفع مبالغ مالية لقاء تجنب هجوم على جهازه أو أجهزته المحوسبة. وبرمجيات الفدية في ازدياد مؤخراً ما دعا بعض المختصين والقانونيين للتحذير من أن أكبر خطر سيواجهه مستخدمو تكنولوجيا المعلومات في سنة ٢٠١٦ هو برمجيات الفدية، والتي تتراوح المبالغ المطلوبة من خلالها ما بين ٢٠٠ و ١٠٠٠٠ دولار [٢٥] و [٢٦].

وإذا استثنينا محاولات القرصنة والابتزاز فإن أمن مثل هذه الأجهزة المحوسبة لا يزال يعتبر محل شك في ظل ضعف الإجراءات المتبعة (من قبل هيئة الـ FDA مثلاً) في ترخيص مثل هذه الأجهزة ما يضعف الوازع لدى المنتجين لاستخدام إجراءات فحص أكثر تشدداً وعدم التسرع في دفع المنتجات إلى السوق قبل فحصها بشكل سليم [٢٣]. وأوضح [٢٧] دور

(٤) تداولت وسائل الإعلام أن نائب الرئيس السابق ديك شيني قد عطل التواصل الشبكي مع جهاز الناظم الذي استخدمه شخصياً، سنة ٢٠٠٧ [١٢].



الأسود في الطائرات لكي لا يمكن التأثير عليه بتاتا، وفي حالة الاختراق يمكن فتح الجهاز ومعرفة الجاني من خلال البيانات المخزنة فيه والتي يجب أن يكون جزءاً منها ما يشبه الأدلة الجنائية [٢٦].

واقترح زو [٢٩] استخدام جهاز خارجي يعمل على التثبيت من هوية المتخاطبين مع الجهاز بهدف منع القرصنة من ذلك التخاطب وبالتالي منع أي تخريب للجهاز أو أي من وظائفه. وأسمى ذلك الجهاز حارس جهاز الـ (IMDGuard). لكن البعض اعترض على الفكرة بدعوى أن الجهاز ثقيل وغير عملي ودعوا لتبني فكرة مشابهة تستبدل الجهاز بالبرمجيات.

ودرس روشانان [٣٠] كل الأبحاث في مجال تأمين الأجهزة الطبية ضد القرصنة، وصنف أنواع المخاطر من الهجمات (وكذلك الحلول) إلى ثلاث اصناف بناءً على الثلاث أجزاء الموجودة في نظم أجهزة الـ IMDs:

- ١ - هجمات على الواجهة الحيوية Telemetry Interface (أي الشبكة اللاسلكية) مثل تلك التي قام بها فو وراغوناثان،
- ٢ - هجمات على (واجهة) المجسات التي تقوم بحساب وتدوين المقاييس الحيوية المستخدمة في تحديد طريقة العلاج، و
- ٣ - هجمات على برمجيات الجهاز التي تحدد كيفية عمله والتي تستطيع تغيير هذه الكيفية سلباً.

وتمثل الدراسات على الهجمات من النوع الأول أغلبية الأبحاث في المجال كما لاحظ روشانان. وقد صنف الحلول للهجمات من النوع الأول إلى أربعة أنواع:

- أ - حلول تستفيد من المقاييس الحيوية Biometrics لتكوين المفاتيح المستخدمة في التشفير.
- ب - حلول تعتمد على المسافة بين المرسل وجهاز الـ IMD كنوع من بروتوكولات التحقق من الهوية.
- ج - حلول تعتمد على بيانات خارجية تقوم بإدارة عمليات التشفير وتحدد طبيعة الـ Authentication.
- د - وحلول تعتمد على جهاز خارجي «يلبس» من قبل المريض ليعمل كحاجز ووسيط بين الـ IMD و المتصلين به ما يحقق الخصوصية والحماية معاً مثل الجهاز المقترح من قبل زو [٢٩] المشروح أعلاه. ويعاب على الفكرة المستوى المنخفض من القبول من جهة المرضى.

إشارات تحكم أبعد من بضعة سنتيمترات كوسيلة للحماية هو سيف ذو حدين. فممنع قبول الإشارات كتأمين ضد القرصنة يؤدي أيضاً لمنع دخول الإشارات الضرورية أيضاً (في حالات الطوارئ مثلاً) حين يحتاج الجهاز لتوجيهات استثنائية من الطبيب المشرف. أولى فو جل عنايته لحل مشكلة نضوب طاقة البطارية بسبب هجمات إنكار الخدمة. كما اهتم أيضاً بإشراك المستخدم في عملية محاربة القرصنة من خلال إيجاد آلية تنبيه في الجهاز. وأخيراً، حاول فو منع أو تثبيط محاولات الهجوم. تمكن فو من تحقيق أهدافه الثلاثة من دون أي تأثير على طاقة البطارية، وصنف جميع الحلول على أنها صفرية الطاقة (لا تستهلك أي طاقة من البطارية) Zero-power defenses وذلك من خلال «حصد» Harvesting الطاقة الناتجة عن إشارات الراديو RF المستعملة في التواصل بين أجزاء النابض والمبرمج وغيره لتحقيق مايلي:

- ١ - لتنبية المستخدم (بالصوت) بوجود حدث له علاقة بأمن الجهاز (مثل هجوم قرصنة)
- ٢ - التحقق من هوية المتداخل مع الجهاز Authentication من خلال عملية تقييم مفاتيح التشفير المتبادلة
- ٣ - تبادل المفاتيح (في عملية التشفير) Key Exchange والتي يستشعرها المستخدم على شكل إهتزازات Vibrations يقوم بها الجهاز.

وأما رادكليف [٩] وأومر [٢٨] وغيرهما من أتباع مبدأ البرامج المجانية المصدر فقد شجعوا مبدأ «القرصنة الإيجابية» التي تهدف لكشف مصدر البرامج المحمية بقوانين حماية الملكية الفكرية للتعديل على أي خطأ أو قصور في تلك البرامج المستخدمة في هذه الأجهزة. وقد أوضح أومر الأسباب التي تجعل مثل هذه البرامج الأجهزة المستخدمة لها أكثر أماناً للأجهزة.

واقترح البعض التحكم الآلي التام في عمليات الأجهزة وتوظيف برمجيات يمكن تعديلها بآخر التحديثات كما يحصل في نظام ويندوز مثلاً. وهذا الاقتراح واجه رفضاً من البعض ممن يملكون أجهزة طبية ترسل ولا تستقبل (Unidirectional) ما يستوجب تدخلاً جراحياً لتغييرها وهو غير محبذ بالطبع. والبعض الآخر اقترح تصميم مثل هذه الأجهزة مثل الصندوق

وجرت العادة أن تقوم هيئة الغذاء والدواء الأمريكية FDA بفحص مطول ومضن لأي أدوية قبل ترخيصها والسماح ببيعها. وعادة ما تقوم الهيئة بعمل ما يسمى قائمة تعليمات ما قبل السوق Pre-market guidelines لتوجيه مصنعي المنتجات الدوائية والغذائية بتصنيع منتجاتهم لتجتاز تلك المجموعة من الفحوصات المضنية في أقل وقت وقبل السماح لأي منتج صحي أو طبي بالظهور في السوق. بعد ظهور المنتج في السوق وبعد مضي فترة كافية تسمح للمستخدمين لهذه المنتجات من تدوين ملاحظاتهم وشكاويهم (إن وجدت)، تقوم الـ FDA بإصدار ما يسمى بتعليمات ما بعد السوق Post market [٢٧]. ولكن هذا التشدد والاهتمام من قبل الـ FDA لا يمكن تلمسه في ما يخص بالأجهزة الطبية المحوسبة. أسباب ذلك كثيرة ومن أهمها عدم وجود مقاييس معيارية للجزء الحاسوبي من الجهاز المطلوب ترخيصه والذي عادة تترك مهمة فحصه لـ «خبراء ومهندسي الحاسب» [٢٣]، فيما تكتفي الـ FDA بوضع الأطر العامة والنصائح [٣]. وهذا لا يعني إهمال الـ FDA لدورها في حماية المستهلك، لكن نقص الكادر المتخصص والضغوطات التي تمارسها المستشفيات ومصانع الأجهزة الطبية وطلبات المستهلكين المتزايدة دفعت الـ FDA للنأي بنفسها عن دور المحقق في هذا الشأن واكتفت بنشر التحذيرات الطبية كلما اكتشف ما يسوغ مثل هذه التحذيرات. فمثلا قامت الـ FDA بنشر تحذير من إمكانية قرصنة مضخات الأنسولين بعد ظهور ذلك في الأبحاث وإهتمام الإعلام (الصحف وقنوات التلفزيون) بهذه القضية [٣٢]. أهمية الموضوع ومسؤوليته تشمل أيضا مهندسي الأجهزة الطبية الحيوية Biomedical Engineers. اقترح وود Wood [٣٣] (كونه يجيد البرمجة وفي نفس الوقت هو مهندس طبي) نهجًا وسيطًا للتقريب بين وجهتي نظر المهندسين و مبرمجي الحاسب للوصول إلى حلول طبية أكثر أمانًا مما هي عليه الآن تشمل تقليل استخدام البرمجيات قدر الإمكان واستخدام وسائل أخرى (مثل المقاييس الحيوية) للثبوت من هوية مستخدم الجهاز، ومقترحات أخرى تركز على أهمية إشراك المهندسين الطبيين لما لتدريتهم المتشدد فيها يخص أمن المريض من دور مأمول في زيادة مستوى الأمان في الأجهزة الطبية المحوسبة.

والحلول القانونية والإجرائية يجب ألا ينتظرها المجتمع

أما في ما يخص الهجمات من النوع الثاني والثالث، فقد لاحظ روشانان قلة عدد الأبحاث التي تعالج المشاكل الناتجة عن سوء تصميم واختبار البرمجيات في الأجهزة، وعددها القليل جدًا في ما يخص الهجمات على المجسات المنشأة للبيانات في هذه النظم. وكلا النوعين خارج عن نطاق بحثنا. لكن من المهم التنبيه على توصيات روشانان بالتعمق في دراسة استخدام البيانات الحيوية كوسيلة متأملة في تكوين مفاتيح التشفير بشكل تفاعلي ومتغير [٣٠].

واستخدم زهانغ [٣١] شبكة النظام الصحي الشخصي PHS كوسيلة لمراقبة أي تغيرات «شاذة» أو غير طبيعية على الأجهزة الطبية المزروعة والتحكم في عملها بناءً على المعلومات المستقاة من هذه المراقبة (مثل تغير مفاجيء في حجم جرعة الدواء دون سبب منطقي). وأطلق زهانج على جهازه اسم MedMon وهو يعمل بنفس طريقة برمجيات مراقبة الشبكة التقليدية المستخدمة من قبل فنيي الشبكات لاكتشاف الخروقات بهدف منعها وتقليل تأثيرها.

وفي ما يخص أمن المرضى في المستشفيات والمراكز الطبية أوصى ناكموب [١٩] بتأمين الشبكات اللاسلكية داخل هذه المباني لمنع القرصنة والتطفل. فيما أوصى جليسون [٢٠] بحماية أجهزة محاكاة الإنسان iStan لأهميتها في تدريب الطواقم الطبية ولاختبارات الاختراق على الأجهزة الطبية المزروعة.

والتوجه العام في ما سبق هو نحو منع القرصنة أو تقليل تأثيرها. لكن هناك توجهًا معاكسًا يشجع القرصنة لمعرفة نص البرامج المستخدمة (من خلال الهندسة العكسية) ليتمكن ذوي الخبرة (وهم كثر) من عمل التعديلات اللازمة على هذه البرمجيات لزيادة فعاليتها ومستوى الأمان فيها. يتبع هذا التوجه الكثير من الناس أغلبهم من المؤمنين بالبرمجيات المفتوحة المصدر Open Source Software. ساندلر Sandler [٦] مثلاً أثبت أن البرمجيات المفتوحة أكثر أمانًا من تلك التجارية (المغلقة المصدر). سمى أومر Omer [٢٨] هذه المجموعات بقرصنة الصحة Health Hackers وأوضح مجموعة من المشاريع على رأسها البنكرياس الصناعي المخصص للأطفال المصابين بالسكري. ويبنى المنتمون لهذا الفكر رأيهم على أن البرامج المفتوحة متاحة للجميع وبالتالي يمكن التعديل عليها أو عمل تطبيقات جديدة (أو تعديل على تطبيقات قائمة) مخصصة لمستخدم معين حسب مستوى معرفته وحاجاته.

القلب ومرض السكري) بشكل آلي، وتستخدم حالياً تطبيقات حاسوبية خاصة تنظم عملها وتبث بيانات قيمة للمشرفين من أطباء وغيرهم للمساعدة في إستمرار عملها بشكل سليم. والانتشار السريع لهذه الأجهزة دون ضوابط قانونية وعلمية كافية، بالإضافة لعوامل أخرى تسبب في الكثير من حالات فشل لهذه الأجهزة نتج عنه إصابات جسدية أو حتى الوفاة في بعض الحالات.

ورغم ندرة التقارير عن وجود حالات قرصنة لمثل هذه الأجهزة وما قد ينتج عنها من تأثيرات، إلا أن الاحتمال النظري لحصول هذا النوع من الهجمات ممكن جداً. فمن المعروف أن أسباب القرصنة الرئيسية تشمل الكسب غير المشروع من خلال الإبتزاز (عادة بواسطة برمجيات الفدية Ransomware)، أو للحصول على متعة الشعور بالانتصار والتغلب على آليات الأمن في هذه الأجهزة. وكلا السببين مسوغ جيد لمحاولات القرصنة<sup>(٥)</sup>.

ومن المهم تذكّر أن الحلول الفنية لوحدها لا تكفي دون أن تتوافر لها القاعدة التشريعية المناسبة لضمان تحققها، وحصول القبول من قبل المستخدمين دون تغيير في كفاءة هذه الأجهزة أو سهولة استخدامها. ومن المشاكل الرئيسية التي أوضحتها البحث عدم توافر معايير قياسية Standards في ما يخص الفحص والترخيص من قبل الهيئات الحكومية المختصة، أو حتى ما يخص البحث والتدريس في المجال. يحث المؤلف على إيجاد مثل هذه المعايير كما يحث على إشراك المرضى والأطباء في كل مراحل تصميم وإستخدام مثل هذه الأجهزة.

والبحث في معظمه كان تلخيصاً للمراجعات الأدبية (الدراسات السابقة) في مجال قرصنة الأجهزة الطبية المصنعة بجسد المريض أو المزروعة داخله WIMDs. وهو بحث نظري (رغم تطرقه للطرق الفنية التي استخدمها أو اقترحها الباحثون)، يرمي إلى التنبيه لخطورة وأهمية موضوع البحث والدراسة فيه ولا يهدف (على الأقل في الوقت الحالي) لتقديم حلول جديدة تمنع قرصنة الأجهزة الطبية أو تخفف من آثارها. كما يهدف إلى تشجيع البحث (والباحث العربي خصوصاً)

(٥) هذا طبعاً بعد استبعاد حالات قرصنة خاصة مثل تلك التي تهدف لاغتيال شخصية عامة أو الانتقام من شخص ما بتخريب جهازه الطبي المزروع أو الملقق.

من هيئة حكومية قد تحكم عملها بيروقراطية تؤدي لعدم تحقيق الأهداف المرجوة، أو ضغوط لوبيات شركات الأدوية والمستشفيات. كما لا يمكن انتظار الحلول الفنية على أساس أنها «الحل» النهائي. فرأي المستهلك مهم جداً ويجب أن يوجه مثل هذه التشريعات والقوانين والإجراءات. في دراسة قامت بها كلية الطب في جامعة واشنطن عن وسائل حماية أجهزة ICD المزروعة، طلب من مجموعة من المرضى اختيار واحدة من مجموعة وسائل لحماية أجهزتهم. كان الجواب الشائع أنه مهما كانت الطريقة المتبعة فيجب أن تتوافر على مجموعة مزايا أهمها أن الطريقة يجب أن تنبه المريض لأي خطر تتعرض له، لكن في نفس الوقت ألا تتطلب التدخل منهم بشكل يحتاجون فيه لمهارات فنية غير متوافرة لديهم (يعني سهولة التحكم والتدخل من قبلهم) ولا أن يضطروا لكشف خصوصيتهم في المقابل [١٣].

وأما أي طريقة فنية يفضل المرضى، فقد أشارت الدراسة إلى أن الغالبية منهم يفضلون الطرق التقليدية مثل الكلمة السرية للتحكم في الجهاز وحمايته من الاختراق. لكن المشكلة كانت في كيفية تدخل الطبيب في حالة غياب المريض عن الوعي وعدم معرفة الطبيب لكلمة السر هذه. حل المشكلة اقترح البعض طباعة كلمة السر على شكل وشم على جسد المريض بشكل لا يظهر إلا للطبيب (بكشفها بالأشعة تحت الحمراء مثلاً). إلا أن أغلب المرضى رفضوا فكرة الوشم وفضلوا عليها فكرة أخرى وهي فكرة الأسورة Bracelet التي تحوي كلمة السر. المشكلة طبعاً كانت في إمكانية ضياع مثل هذه الأسورة [١٣]. وتخلص الدراسة إلى أن الحلول يجب أن تكون مقبولة من قبل المستخدم وإلى ضرورة وجود مقاييس معيارية تستخدمها الجهات المشرفة والمرخصة، وتلتزم بها الجهات المصنعة لهذه الأجهزة.

## الخاتمة

نوقش في هذا البحث موضوع إمكانية قرصنة الأجهزة الطبية المزروعة (منظمات ضربات القلب المحوسبة ICD تحديداً) أو المصنعة بالجسد البشري (نظام ضخ الأنسولين المحوسب تحديداً) والحلول الفنية المناسبة لمنع مثل هذه القرصنة أو التخفيف من آثارها. وتهدف الأجهزة مدار البحث للعمل على علاج أمراض مزمنة (عدم انتظام ضربات

- 7.C. Israel and S. Barold, "Pacemaker systems as implantable cardiac rhythm monitors," American Journal of Cardiology, volume 88, no. 4, pp. 442–445, Aug. 2001.
- 8.Z. Guanglou et al., "Ideas and Challenges for Securing Wireless Implantable Medical Devices: A Review," Article in IEEE Sensors Journal, no. 99, December 2016.
- 9.J. Radcliffe, "Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System," in Proc. Black Hat Technical Security Conference, Jul./Aug. 2011.
- 10.M. Tobias, "What to stop hackers from infecting Medical Devices", Forbes Magazine, April 2012, Online: <http://www.forbes.com/sites/marcwebertobias/2012/04/20/whats-to-stop-hackers-from-infecting-medical-devices/3/#6c12ff6a1b87>.
11. Gift of fire: Social, Legal, and Ethical Issues for computing Technology. Sara Baase. 4<sup>th</sup> edition, Pearson Education/Prentice Hall Publications, 2013.
- 12.D. Clery, "Could a wireless pacemaker let hackers take control of your heart?", Science magazine, February 2015, online: <http://www.sciencemag.org/news/2015/02/could-wireless-pacemaker-let-hackers-take-control-your-heart>.
- 13.N. Leavitt, "Researchers Fight to Keep Implanted Medical Devices Safe from Hackers," IEEE Computer Society, Technology News, August 2010.
- 14.T. Martin, M. Hsiao, D. Ha, and J. Krishnaswami, "Denial-of-service attacks on battery-powered mobile computers," in Proc. IEEE Conference on Pervasive Computing and Communications, pp. 309–318, March 2004.
- 15.E. Haselsteiner and K. Breitfuss, "Security in near field communication," in Proceedings of the Workshop on RFID Security, pp. 3–13, July 2006.
- 16.D. Hayes et al., "Interference with cardiac pacemakers by cellular telephones," New England Journal of Medicine., volume 336, no. 21, pp. 1473–1479, May 1997.
- 17.S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in Proceedings of ACM International

في مجال تأمين الأجهزة الطبية المصققة أو المزروعة في جسد الإنسان. القائمة التالية تمثل مجموعة غير حصرية من الأسئلة المفتوحة والقابلة للبحث:

- ١ - موازنة الفعالية مع الأمان في الأجهزة الطبية المصققة أو المزروعة.
- ٢ - ترخيص الأجهزة الطبية المصققة أو المزروعة.
- ٣ - التشفير كوسيلة تأمين لاتصالات الأجهزة الطبية المصققة أو المزروعة.
- ٤ - توفير الأدلة الجنائية الرقمية في الأجهزة الطبية المصققة أو المزروعة وتحليلها.
- ٥ - استخدام وسائل تحليل البيانات الحديثة وتكنولوجيا البيانات الكبيرة Big Data والسحب الرقمية في تسريع إيجاد حلول للمشاكل المذكورة أعلاه.

## المراجع

- 1.K. Saleem et al, "Survey on Cybersecurity Issues in Wireless Mesh Networks based eHealthcare", IEEE 18<sup>th</sup> International Conference on e-Healthcare Networking, Applications, and Services, 2016.
- 2.M. Zhang, A. Raghunathan, and N. K. Jha, "MedMon: Securing medical devices through wireless monitoring and anomaly detection," IEEE Transactions in Biomedical Circuits Systems, volume 7, no. 6, pp. 871–881, Dec. 2013.
- 3.A. Burns, M. Johnson, and P. Honeyman, "Brief Chronology of Medical Device Security," Communications of the ACM, volume 59, no. 10, October 2016.
- 4.K. Fu et al, "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses," in Proceedings of the IEEE Symposium on Security and Privacy, pp.129-142, May 2008.
- 5.Google Images of ICDs. Online: <https://www.google.com.sa/search?safe=strict&hl=ar&site=imghp&tbm=isch&source=hp&biw=1280&bih=633&q=implantable+cardioverter+defibrillator&oq=Implantable&gs>.
- 6.K. Sandler, L. Ohrstrom, L. Moy, and R. McVay, "Killed by Code: Transparency in Implantable Medical Devices," 2010. Online: <http://www.softwarefreedom.org>.



- 29.F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IM-DGuard: Securing implantable medical devices with the external wearable guardian," in Proceedings of the IEEE International Conference on Computer Communications, pp. 1862–1870, April 2011.
- 30.M. Rushanan, A. Rubin, D. Kune, and C. Swanson, "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks," IEEE Symposium on Security and Privacy, 2014.
- 31.M. Zhang, A. Raghunathan, and N.K. Jha, "Trustworthiness of Medical Devices and Body Area Networks," Proceedings of the IEEE, volume 102, no. 8, August 2014.
- 32.A. Ossola, "FDA issues warning about hackable Medical Devices", Popular science magazine, August 2015, online: <http://www.popsci.com/fda-issues-warning-cyber-security-risks-medical-devices> .
- 33.B. Wood, "Medical Device Security: A Biomedical Engineering Professional's Perspective," Information Systems Security Association (ASSA) Journal, pp. 14-17, September 2014.
- 18.C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in Proceedings of the IEEE International Conference on e-Health Networks Applied Services, June 2011.
- 19.J. Knackmuß, T. Möller, and R. Creutzburg, "Security risk of medical devices in IT networks: the case of an infusion pump unit," in Proceedings of the International Society for Optical Engineering (SPIE), March 2015.
- 20.W. Glisson et al., "Compromising a medical Mannequin," Cornell University Library, [Online] [www.arXiv.org/abs/1509.00065](http://www.arXiv.org/abs/1509.00065), August 2015.
- 21.D. Storm, "Researchers hack a pacemaker, kill a man (nequin)", Computer World, September 2015, Online: <http://www.computerworld.com/article/2981527/cybercrime-hacking/researchers-hack-a-pacemaker-kill-a-mannequin.html> .
- 22.iStan from CAE healthcare, a pdf file, online: [www.caehealthcare.com](http://www.caehealthcare.com) .
- 23.W. Maisel and T. Kohno, "Improving the Security and Privacy of Implantable Medical Devices," New England Journal of Medicine, volume 362, no.13, pp. 1164-1166, April 1st, 2010.
- 24.D. Basulto, "From Hacking Computers to Hacking Humans", Big Think, January 2016, online: <http://bigthink.com/endless-innovation/from-hacking-computers-to-hacking-humans> .
- 15.A. Ossola, "Hacked Medical Devices may be the biggest cybersecurity threat in 2016", Popular science, November 2015, online: <http://www.popsci.com/hackers-could-soon-hold-your-life-ransom-by-hijacking-your-medical-devices> .
- 26.J. Porup, "Ransomware is coming to Medical Devices", Motherboard Magazine, November 2015, online: <http://motherboard.vice.com/read/ransomware-is-coming-to-medical-devices> .
- 27.D. Kramer et al., "Security and Privacy Qualities of Medical Devices: An Analysis of FDA Post-market Surveillance," Los Angeles Biomedical Research Institute, PlosOne open access article, July 2012.
- 28.T. Omer, "Empowered citizen 'health hackers' who are not waiting," BioMedCentral Journal, volume 14, no. 118, August 2016.

## ملخص السيرة الذاتية



د. محمد سعيد غزال

البريد الإلكتروني

mohammed.ghazal@nauss.edu.sa

السجل الأكاديمي:

- حاصل على درجة الدكتوراه في نظم المعلومات الحاسوبية سنة ٢٠١١، ودرجة الماجستير في نفس التخصص من جامعة ديپول في الولايات المتحدة سنة ٢٠٠١.
- حاصل على درجة الماجستير في اقتصاد الطاقة والمعادن من جامعة تكساس ١٩٩٣.
- حاصل على درجة البكالوريوس في هندسة التعدين من جامعة الملك فهد للبترول والمعادن سنة ١٩٨٥.

سجل العمل الأكاديمي:

- ٢٠١٤ وحتى الآن: أستاذ مساعد في قسم الدراسات الأمنية بكلية العدالة الجنائية في جامعة نايف العربية للعلوم الأمنية. عمل في كلية أمن الحاسب والمعلومات لستين، وحاليا يعمل كمشرف علمي على برنامج دبلوم الجرائم الإلكترونية في كلية العدالة الجنائية.
- ٢٠٠٢-٢٠١٤: عمل كأستاذ مساعد في نظم المعلومات الحاسوبية ونظم المعلومات الادارية في عدة جامعات في السعودية والأردن والإمارات تشمل الجامعة الأردنية وجامعة عمان الأهلية وجامعة أبوظبي وجامعة العين.
- ١٩٩٠-٢٠٠١: عمل في عدة جامعات وكليات جامعية في الولايات المتحدة الأمريكية كمدرس في الحاسب الآلي والرياضيات.

سجل البحث العلمي:

- ألف كتابا في نظم المعلومات الادارية سنة ٢٠٠٣.
- كتب في مجال تنقيب البيانات Data Mining وتحديد عنايق البيانات Clustering وتوظيف ذلك في مجال محاربة عمليات الاحتيال وتأمين نظم المعلومات.
- اهتماماته البحثية حاليا: أمن نظم المعلومات الصحية والأجهزة الطبية المحوسبة، المقاييس الحيوية، والبحث الجنائي الرقمي.