

Medical Device Security

Gruppe 9

Lucas Garzarolli, 0955824,

David Eigenstuhler, 1257180,

Paul Wörtl, 0857021,

Gerald Zauner, 0756323

Institut für Wirtschaftsinformatik

Software Engineering

Johannes Kepler Universität Linz

Service Engineering SE (259.039 / WS 2014)

LVA Leiter: a. Univ.-Prof. Dr. Johannes Sametinger

18.12.2014

Inhaltsverzeichnis

1	Einleitung	1
2	Effiziente Ressourcennutzung und Sicherheit	2
2.1	Sichere und energieeffiziente Netzwerkkommunikation	3
2.2	Ein energieeffizientes Sicherheitsprotokoll	4
3	Allgemeine und spezielle Sicherheitsziele	6
3.1	Normen für die Sicherheit von Medizinprodukten	8
3.2	Definition von Informationssicherheit	9
4	Angriffsarten und Angriffspfade	11
4.1	Sicherheitsangriffe	12
5	Kategorien von Geräten und Scope	13
6	Klassifizierung	13
6.1	Biomedizinische Technik	14
6.2	Medizin	15
6.3	Informationssicherheit	15
6.4	Klassifikation der Auswirkungen	16
6.5	Klassifikation der Verwundbarkeit	16
6.6	Folgen	17
7	Sicherheitsmaßnahmen, Vorkehrungen und Verteidigungsstrategien	18
7.1	Präventive Maßnahmen	19
7.2	Aspekte der Betriebssicherheit und Anwendbarkeit	19
7.3	Aspekte zu Maßnahmen zur Erreichung von Sicherheitszielen und Privatsphäre	20
7.4	Aspekte der Kommunikation	22
8	Fazit, Zusammenfassung und Ausblick	24

Literatur	25
-----------------	----

1 Einleitung

Heutzutage sind Wireless Sensor Networks (WSNs) allgegenwärtig und werden in einer Vielzahl von Anwendungsgebieten eingesetzt. Im letzten Jahrzehnt fand diese Technologie auch weitgehende Verbreitung im Bereich medizinischer Diagnosesysteme. Medizintechnische Geräte, die verwendet werden um WSNs einzurichten können prinzipiell in implantierbare und externe Geräte unterteilt werden. Wobei Erstere dazu genutzt werden um spezifische Messungen im Körper des Patienten durchzuführen und somit dessen Gesundheit zu überwachen. Diese Daten werden an externe Geräte übermittelt, welche diese Informationen sammeln, verarbeiten und gegebenenfalls Maßnahmen einleiten um auf gesundheitskritische Ereignisse zu reagieren. (Daniluk & Niewiadomska-Szynkiewicz, 2012)

Auf Grund der zunehmenden Verbreitung von WSNs im medizinischen Bereich konzentriert sich auch die Forschung verstärkt auf die Entwicklung von sicheren und stabilen Netzwerksystemen für medizinische Diagnosezwecke. Häufig eingesetzte implantierbare medizintechnische Geräte (IMGs), wie zum Beispiel Herzschrittmacher, Blutzuckermessgeräte und damit verbundene Insulinpumpen können eine Art Sensornetzwerk in unserem Körper bilden, welches im Vergleich zu anderen WSNs von spezifischen Einschränkungen betroffen ist. Daher müssen bei der Entwicklung von IMGs bestimmte Aspekte bezüglich der Stabilität, Sicherheit und der Energieressourcen beachtet werden. (Grimes, 2004)

Für die Entwicklung eines stabilen und sicheren Systems gilt es die Architektur mit spezifischen Lösungen zu erweitern, um die Kommunikationskanäle abzusichern und das System vor der Abhörung, Einbringung oder Modifikation der zu übermittelnden Daten zu bewahren. In den folgenden Kapiteln werden wir auf sicherheitsrelevante Aspekte, im Kontext der speziellen Merkmale von IMGs, eingehen und die damit verbundenen Herausforderung an das System, beziehungsweise dessen Entwurf, diskutieren.

2 Effiziente Ressourcennutzung und Sicherheit

Implantierbare medizintechnischen Geräte (IMGs) ermöglichen Patienten sich frei zu bewegen und ihren Alltag mit möglichst geringen Einschränkungen zu beschreiten, während die Möglichkeit besteht ihren Gesundheitsstatus kontinuierlich zu überwachen. (Hosseini-Khayat, 2011)

IMGs können basierend auf deren Energieversorgung prinzipiell in zwei Gruppen unterteilt werden:

- Geräte mit integrierten, nicht wiederaufladbaren Batterien (z.B.: Herzschrittmacher)
- Geräte die induktiv betrieben werden (z.B.: Cochleaimplantat)

Wobei die meisten IMGs prinzipiell aus Sensoren und Funkverbindungs-Modulen bestehen, welche mittels einer Batterie mit Strom versorgt werden. Da die Wartung dieser Geräte einen chirurgischen Eingriffes erfordert und sich somit sehr aufwendig gestaltet, gilt es die Energieeffizienz zu optimieren und die Lebensdauer der Batterien zu maximieren. Dieser Aspekt sollte auch bei der Entwicklung des Sicherheitskonzepts berücksichtigt werden, das die Grundlage für eine zuverlässige und vertrauliche Datenübertragung bildet und die Geräte vor unbefugten Zugriffen schützt. Des Weiteren ist, auf Grund der kabellosen Übertragung, ebenfalls die Übertragungsrate von IMGs eingeschränkt. Um die Zeitfenster für potentielle Störungen und Eingriffe zu minimieren, sowie Energie zu sparen, sollte die Übertragung der Bits möglichst schnell abgeschlossen und somit auch die eingesetzte Hardware sorgfältig ausgewählt werden. (Daniluk & Niewiadomska-Szynkiewicz, 2012)

Die derzeitig verfügbaren IMGs stellen diverse Funktionalitäten zur Verfügung, wobei die Folgenden am verbreitesten sind:

- das Monitoring bestimmter körperlicher Funktionen und Aktivitäten,

- die Steuerung und direkte Programmierung, sowie indirekte Programmierung der IMGs über das Internet,
- die automatische oder gesteuerte Verabreichung von bestimmten Dosen eines Medikaments,
- sowie die Möglichkeit Informationen bezüglich der Implantate direkt vom Gerät anzufordern (Daniluk & Niewiadomska-Szynkiewicz, 2012).

2.1 Sichere und energieeffiziente Netzwerkkommunikation

Mit Sicherheitsaspekten auf der einen Seite und Energieeffizienz auf der anderen Seite stehen sich zwei konkurrierende Ziele gegenüber, wobei jedoch keines der beiden vernachlässigbar ist - daher gilt es einen Kompromiss zu finden. Im Folgenden werden theoretische Ansätze diskutiert, deren Schwerpunkt auf der Bereitstellung eines sicheren und energieeffizienten Netzwerks liegt.

Wie bereits erläutert handelt es sich bei IMGs vereinfacht um Geräte, die aus Sensoren und Modulen zur Realisierung der Funkverbindung bestehen, die in den menschlichen Körper eingesetzt werden. Die Messwerte werden zu einer externen Basisstation übertragen, die sich am Körper des Patienten, beziehungsweise an dessen Kleidung, befindet. Die gesammelten Daten werden von der Basisstation an ein mobiles Gerät übermittelt, welches die Rolle eines Brokers zwischen dem Patient und dem behandelnden Arzt einnimmt. (Daniluk & Niewiadomska-Szynkiewicz, 2012)

Ein möglicher Ansatz ist die Entwicklung eines externen Sicherheitsgeräts, welches gegebenenfalls auch in die Basisstation integriert werden könnte. Dieses Gerät wäre dafür verantwortlich die Kommunikation zwischen den Sensoren und der Basisstation zu überwachen und auffälliges Verhalten im Sensorennetzwerk zu identifizieren, mit dem Ziel unzulässige Kommunikation zu unterbinden und somit Angriffe weitgehend abzublocken. Verhalten kann mittels

im Vorhinein definierter oder dynamisch erlernter Regeln überprüft werden. Durch das Blockieren unzulässiger Übertragungen wird es ermöglicht die Batterie des IMGs zusätzlich zu entlasten und somit deren Lebensdauer zu erhöhen. (Daniluk & Niewiadomska-Szynkiewicz, 2012)

Außerdem wäre es sinnvoll einen Mechanismus zur Aggregation von Messdaten anzuwenden, wodurch redundante Information eliminiert und Energieressourcen eingespart werden könnten. Um die Aggregation sicher gestalten zu können sind eine Authentifizierung, sowie die Vertraulichkeit und Integrität der Daten obligatorisch, wobei wohl überlegt werden muss wie diese zu implementieren ist um effizient zu laufen. Des Weiteren ist es möglich durch die Reduktion der Signalstärke und somit der Reduktion der Funkreichweite, Angriffe auf das System zusätzlich zu erschweren, da potentielle Angreifer physisch näher an das Gerät heran müssen um die IMGs ansprechen zu können. In Verbindung mit einer optimierten Positionierung der Sensoren und des Senders kann der Energieverbrauch weiter optimiert werden. Derzeit werden in Experimenten die optimalen Konfigurationen ermittelt. (Daniluk & Niewiadomska-Szynkiewicz, 2012)

2.2 Ein energieeffizientes Sicherheitsprotokoll

Solide und bewährte Sicherheitsmechanismen, wie die asymmetrische Verschlüsselung, können hohe Kosten hinsichtlich der Rechenzeit und des Energiekonsums verursachen. Somit stehen sich auf der einen Seite mit der Verwendung kryptografischer Methoden zur Sicherung des Übertragungskanals und auf der anderen Seite mit der Langlebigkeit, sowie der Performance des IMGs konkurrierende Ziele gegenüber. Folgend wird ein Sicherheitsprotokoll präsentiert, dass einerseits energieeffizient ist und andererseits einen angemessenen Grad an Sicherheit bietet.

Für das Sicherheitsprotokoll werden folgende Ziele definiert:

- Vertraulichkeit: unbefugte Dritte können gesendete Nachrichten nicht lesen,
- Autorisierung: Nachrichten von unautorisierten Dritten werden erkannt und abgewiesen,
- Integrität: Nachrichten können nicht von Dritten manipuliert werden,
- sowie keine Wiederholbarkeit: ordnungsgemäße Nachrichten können nicht von Dritten unrechtmäßig repliziert und erneut gesendet werden (Hosseini-Khayat, 2011).

Im Folgenden wird erläutert, wie diese Ziele effizient und ressourcensparend erreicht werden, zuerst wird auf Voraussetzungen eingegangen und dann das Grundprinzip des Protokolls erläutert. Eine leicht zu implementierende Alternative zur asymmetrischen Verschlüsselung ist die symmetrische Kryptographie, da in jedem Fall ein physischer Kontakt zwischen dem Patienten und dem behandelnden Arzt stattfindet, stellt auch die vertrauliche, physische Übergabe eines Schlüssels kein Problem dar. Das hier vorgestellte Konzept sieht eine ebensolche symmetrische Verschlüsselung zwischen dem IMG und der Basisstation, zu der die Messdaten übertragen werden, vor. Der symmetrische Schlüssel wird hierbei auf dem implantierten Gerät gespeichert und vertraulich zur Konfiguration der Basisstation an den behandelnden Arzt und den Patienten weitergegeben. (Hosseini-Khayat, 2011)

Eine Schlüssellänge von 80 Bit und Datenblock-Größe von 64 Bit sind speziell an die Anforderungen von IMGs angepasst. Zur Entschlüsselung wird ein 64 Bit ultra-lightweight Block Cipher Decryptor verwendet. Weiters verfügt jedes implantierte Gerät über eine abgespeicherte 32 Bit lange Seriennummer, die unter allen IMGs, die das gleiche Protokoll verwenden, eindeutig ist. Das IMG und die Basisstation haben einen Zähler der mit 0 initialisiert wird und ebenfalls eine Länge von 32 Bit hat, bei jeder gesendeten Nachricht wird er um eins erhöht - wodurch Nachrichten von unbefugten Dritten nicht repliziert werden können. (Hosseini-Khayat, 2011)

Das Grundprinzip des Protokolls ist simpel gehalten. Anstatt einer gewöhnlichen Authentifizierung werden zwei Zähler verwendet, einer im IMG und einer in der Basisstation. Bei

jedem Sendevorgang wird der Zähler der Basisstation erhöht, wenn der Zähler der Basisstation höher ist, als jener des implantierten Geräts wird die Nachricht angenommen und der Zähler der des IMGs auf den Wert des anderen Zählers gesetzt, somit kann ausgeschlossen werden, dass Nachrichten wiederholt werden. Durch die Verschlüsselung der Nachrichten kann das Auslesen des Zählers, beziehungsweise die Manipulation der Nachricht, ausgeschlossen werden. Außerdem wird durch diese Methode gewährleistet, dass das System nicht neu synchronisiert werden muss, wenn eine Nachricht verloren geht. Da das implantierte Gerät lediglich einen Zähler und einen Vergleichsmethode benötigt, wird nur sehr wenig Rechenleistung in Anspruch genommen. Um die Sicherheit zu erhöhen ist es optional möglich den Zähler jeweils um eine kleine Zufallszahl zu erhöhen. (Hosseini-Khayat, 2011)

Das Protokoll ist so ausgelegt, dass so wenig Hardware Module als möglich verwendet werden. Durch den Einsatz eines ultra-lightweight Block Cipher, wie zum Beispiel PRESENT-80, kann der Einsatz eines energie-ineffizienten Random-Access Memories vermieden werden um die beschriebenen Operationen durchzuführen. (Hosseini-Khayat, 2011)

Basierend auf der minimalistisch gehaltenen Logik und den sorgfältig ausgewählten Hardware Komponenten, wird ein Protokoll geboten, welches im Hinblick sowohl auf die Sicherheitskomponente als auch bezüglich der Energieeffizienz als ausreichend angesehen werden kann.

3 Allgemeine und spezielle Sicherheitsziele

Die Themen Sicherheit und Risiko rücken immer dann in den Mittelpunkt des öffentlichen Interesses, wenn durch Fehler in Geräten oder technischen Systemen Menschen zu Schaden gekommen sind. Gefahren und Unfälle können durch menschliches Versagen ausgelöst werden, aber auch durch technische Defekte in Systemen unterschiedlichster Art. Systeme die nicht vor Missbrauch geschützt werden oder auch andere sicherheitstechnischen Schwächen aufzeigen,

sind nicht sicher und stellen ein erhöhtes Risiko für Personen dar. [Löw, Pabst Petry 2010, S. 9]

Benutzer von technischen Geräten haben verständlicherweise sehr hohe Erwartungen an die Sicherheit von Systemen und die Reduzierung der Risiken und Defekten. Hersteller wollen sichere Produkte kostengünstig entwickeln durch Unfälle vermeiden und die Kundenzufriedenheit erhalten. [Löw, Pabst Petry 2010, S. 10]

In den vergangenen Jahren ist der Anteil der sicherheitsbezogenen, elektronischen Steuerungen und der Software in den verschiedenen Produkten stark angestiegen. Daraus ergibt sich natürlich eine wachsende Komplexität der Systeme und Anforderungen an die Sicherheit der Geräte. In aktuellen Kraftfahrzeugen finden sich schon bis zu 80 verschiedene elektronische Steuergeräte die für Sicherheit der Passagiere sorgen. Diese Entwicklung spiegelt sich jedoch in fast allen Bereichen wieder, unter anderem auch bei Medizingeräten. Im Bereich der Medizintechnik spielt das Thema Sicherheit und Zuverlässigkeit eine sehr wichtige Rolle. Die Software in diesen Chips, die zu einem sicheren Betrieb der Geräte beiträgt, muss dann jedoch stabiler und zuverlässiger funktionieren als etwa das Betriebssystem eines heutigen Laptops, das den Betrieb ab und zu durch einen Neustart unterbricht, wenn es meint, überlastet zu sein. [Löw, Pabst Petry 2010, S. 10]

Um Anforderungen an Sicherheiten von Produkten erfüllen zu können, ist die Anwendung von Sicherheitsnormen dringend erforderlich. Diese Normen beschreiben Standards, welche von der Mehrzahl der Fachleute als korrekt anerkannt wird und sich auch in der Praxis gut bewährt hat. Die Anwendung der Regeln unterstützt zusätzlich die nachweisbare Erfüllung der Sicherheitsanforderungen an Produkte. [Löw, Pabst Petry 2010, S. 11]

3.1 Normen für die Sicherheit von Medizinprodukten

Einen Stand der Technik widerspiegelndes Dokument definiert sich als Norm. Eine Norm regelt und erleichtert somit durch Festlegungen allgemeine und wiederkehrende Anwendungen, wie zum Beispiel Herstellungsprozesse, Prüfverfahren, sowie Produkteigenschaften. Sie können sich somit sowohl auf Gegenstände als auch auf Verfahren beziehen. [Rölleke 2010, S. 605]

Normen haben für sich genommen keinerlei Gesetzeskraft. Ihre Anwendung für Produkte, Hersteller, Betreiber und Anwender ist somit freiwillig. Erst durch Rechtsakte können Normen Verbindlichkeit erlangen, etwa wenn auf sie in privaten Verträgen oder in Gesetzen und Verordnungen Bezug genommen wird. [Rölleke 2010, S. 606]

Nun wollen wir auf Normen in Bezug auf Medizinprodukte näher eingehen. Ein Medizinprodukt ist ein einzelnes oder mit anderen Medizinprodukten verbundenes Instrument, Apparat oder Vorrichtung, welche einschließlich der für ein einwandfreies funktionierendes Medizinproduktes eingesetzte Software, die vom Hersteller zur Anwendung für Menschen mittels ihrer dafür vorgesehenen Funktionen benutzt wird. Die Einhaltung grundlegender Anforderungen bei medizinischen Produkten ist nach der jeweiligen Europäischen Richtlinie zu erfüllen. [Rölleke 2010, S. 606]

Für alle Medizinprodukte gilt die „DIN EN ISO 14971“. Da diese Norm, als Prozessstandard noch die größte Produktnähe aufweist, wollen wir sie an dieser Stelle etwas näher darauf eingehen. Die Norm „DIN EN ISO 14971“ wurde spezifisch für die Herstellung von Medizinprodukten entwickelt und behandelt sich mit dem Erkennen, Bewerten und Minimieren von Risiken, die natürlich in der erster Linie Patienten betreffen könnten. [Rölleke 2010, S. 607]

Das Risiko lässt sich, neben subjektiv geprägten Parametern, auch durch folgende 2 Faktoren charakterisieren:

- Wahrscheinlichkeit des Auftretens eines Schadens
- Auswirkung des Schadens

Die Risikomanagementnorm „DIN EN ISO 14971“ kann ebenfalls Prozesse zur Identifizierung und Minimierung von Gefährdungen festlegen, die von Medizinprodukten ausgehen können. Einen Risikobereich vertretbar konkretisieren ist pauschal jedoch nicht möglich. [Rölleke 2010, S. 608]

Wie schon zuvor erwähnt beschreibt die Norm „DIN EN ISO 14971“ eine Risikomanagementnorm bzw. ein Verfahren. Die Abbildung 1 zeigt den, die in der ISO 14971 festgelegten, Risikomanagementprozess. Es gibt 4 Schritte für das Risikomanagement, welche zu beachten sind. [Rau 2010, S. 129]

- Risikoanalyse (risk analysis)
- Risikobewertung (risk evaluation)
- Risikokontrolle (risk control)
- Postproduktionsinformationen (post-production information)

3.2 Definition von Informationssicherheit

Der weiter verbreitete Begriff der IT-Sicherheit erfüllt nicht mehr die Anforderungen einer ganzheitlichen Betrachtungsweise, da Geräte aus dem mobilen Bereich (wie in etwas Smartphones) nicht als IT-Systeme bzw. IT-Geräte verstanden werden und dadurch oft übersehen werden. Aus dieser Gegebenheit heraus, ist es normgerechter den Begriff Informationssicherheit zu verwenden. [Vogel, Gruetz 2010, S. 163]

Unter dem Begriff Informationssicherheit versteht man im Wesentlichen folgende Punkte:

- Vertraulichkeit

Die Informationen werden nur den dazu befugten Personen zugänglich gemacht.

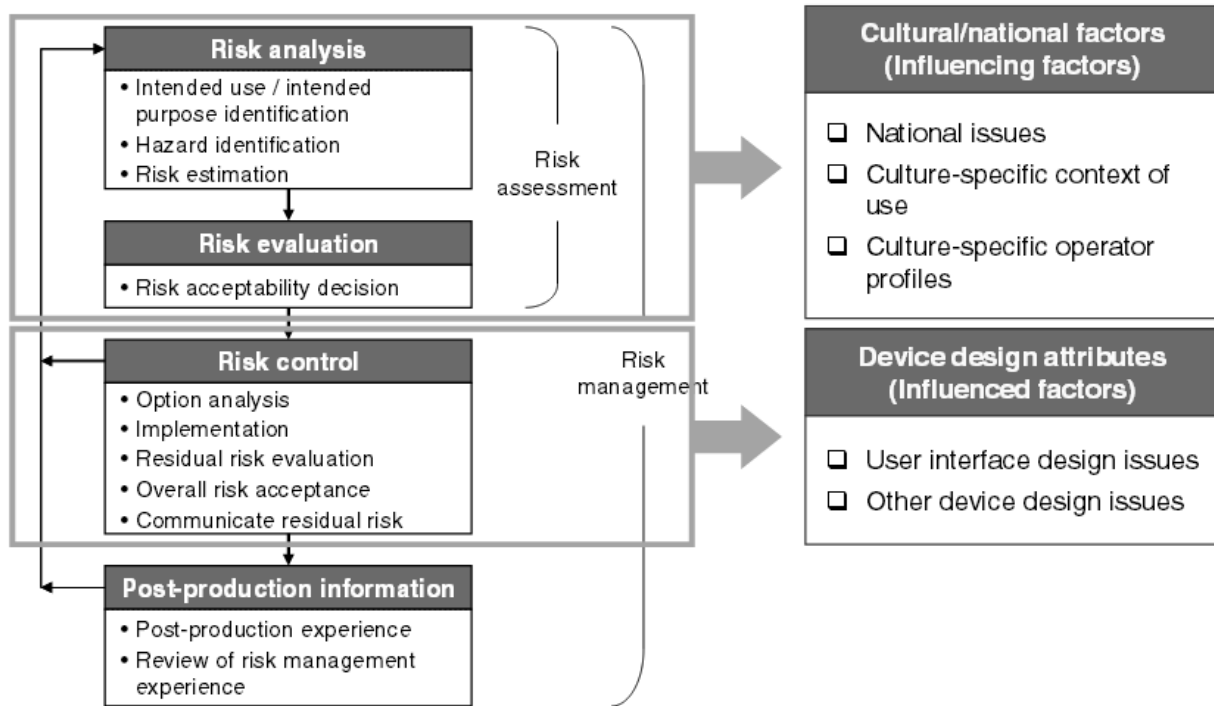


Abb. 1. Riskomanagement and Faktoren für kulturübergreifende Gestaltung von Medizinprodukten [Rau 2010, S. 129]

– Verfügbarkeit

Die Informationen sind in angemessener Zeit aufrufbar.

– Integrität

Die Informationen bleiben richtig und vollständig.

– Zurechenbarkeit

Die Änderungen der Informationen kann dem Urheber der Änderungen zugerechnet werden.

– Authentizität

Der Systembenutzer oder das System selbst ist tatsächlich derjenige bzw. dasjenige für den er oder es sich ausgibt.

Informationssicherheit dient der Aufrechterhaltung des Geschäftsbetriebs. In weiterer Folge werden dadurch auch die Geschäftsrisiken minimiert und die Rendite und Geschäftschancen

zen maximiert. Informationssicherheit ist somit der Schutz von Informationen vor einer Vielzahl von unternehmerischen Bedrohungen. [Vogel, Gruetz 2010, S. 163]

Die Informationssicherheit unterstützt somit das Unternehmen und darf nicht als Hindernis angesehen werden. Welche Sicherheitsziele nun gelten, also beispielsweise welches Maß an Vertraulichkeit bzw. Verfügbarkeit für die Informationen gelten soll, sollte jedes Krankenhaus verbindlich und hausweit gültig in den Sicherheitslinien festlegen. Folgende Ziele könnten in die Sicherheitslinien festzuschreiben sein:

- Unternehmenswichtige IT-Systeme sind hoch verfügbar
- Alle Systeme werden von einem Zugriff durch Unbefugte geschützt
- Die Anforderungen an die ärztliche Schweigepflicht werden eingehalten
- Kosten für die Geschäftsprozesse werden optimiert
- Schadensfälle durch nicht gesicherte IT-Systeme werden unterbunden

[Vogel, Gruetz 2010, S. 163]

4 Angriffsarten und Angriffspfade

Immer mehr klassische Medizingeräte werden durch neuere innovative Geräte ersetzt, deren Funktionalität durch Software gesteuert wird und die zum Austausch von Daten über das LAN (Local Area Network) oder WLAN (Wireless Local Area Network) kommunizieren. Diese Geräte wachsen in die IT eines Krankenhauses hinein und unterliegen somit auch deren Gefahrenpotential. In den letzten Jahrzehnten waren in fast allen Häusern die Bereiche IT und Medizintechnik klassisch getrennt. In den letzten Jahren werden doch immer öfters herkömmliche PCs zur Steuerung bzw. Auswertung der Daten von Medizingeräte. Auch fordert das Krankenhauspersonal erfasste Daten möglichst überall im Haus verfügbar zu haben. Hierbei wird oft auf eine gemeinsam genutzte LAN-Kabel-Infrastruktur zurückgegriffen. Dabei ergeben sich jedoch folglich einige Sicherheitsprobleme. [Vogel, Gruetz 2010, S. 162]

Die Medizintechnik, die bisher quasi, in einer sicheren Umgebung arbeiten konnte, hatte bisher keinerlei bösartige Ein- und Angriffe zu erwarten, da es sich meist um nicht vernetzte Geräte handelte. Diese Geräte waren zusätzlich auch noch mit proprietären Betriebssystemen ausgestattet oder in abgeschlossenen Netzen ohne Zugang zur Außenwelt, geschweige denn zum Internet. Auf der anderen Seite haben wir die moderne IT, die seit Jahren mit Viren und Trojanern, mit Fehlern in Betriebssystemen und Software leben muss. Dadurch hat sich ein reichhaltiges Wissen zur Gefahrenabwehr angehäuft. [Vogel, Gruetz 2010, S. 162]

4.1 Sicherheitsangriffe

Aus der Gegebenheit heraus, dass in Krankenhäusern dieselben bis sehr ähnliche IT-Infrastrukturen wie in anderen Unternehmen zum Einsatz kommen, ergeben dieselben klassischen IT-Sicherheitsprobleme und Angriffsarten.

- Routing Protocoll Injection

Hierbei wird unbefugt die Routingtabelle von Gatewaysystemen verfälscht

- Denial-of-Service-Angriffe

DoS-Angriffe unterscheiden sich in einem Punkt von anderen Angriffsarten. Bei dieser Art des Angriffs will der Angreifer nicht Zugang zum Netzwerk, sondern der Angriff hat den Zweck das System so stark zu überlasten, dass eine normale Nutzung nicht mehr möglich ist.

- Die Anforderungen an die ärztliche Schweigepflicht werden eingehalten

- IP-Spoofing Angriff

Hierbei wird unter Vortäuschung einer falschen IP-Adresse Aktionen gegen fremde Systeme gestartet. Durch die Identitätsverschleierung ist es oftmals schwierig den Verursacher zeitnah zu identifizieren.

- Password Cracking Angriffe

Dies stellt wohl die gebräuchlichste Form von Angriffe auf IT-Systeme dar. Es wird versucht Zugänge auf dem Zielsystem und die zugehörigen Passwörter zu ermitteln.

- Man-in-the-middle-Angriff

Dies ist eine Angriffsart bei der sich eine initialisierende Kommunikationsbeziehung, bei der sich der Angreifer logisch genau zwischen den Partner befindet. Es wird dem Angreifer somit möglich sein, Daten mitzulesen und ggf. auch zu manipulieren. Die Sicherheit kann in diesem Zusammenhang erhöht werden, wenn sich beide Partner einer starken Authentifizierung beim Verbindungsaufbau unterziehen müssen.

[Laszlo 2004, S. 14]

5 Kategorien von Geräten und Scope

Eine Vielzahl an implantierbaren medizinischen Geräten existiert bereits. Wurden in dieser Branche des US Marktes 2010 bereits 32,3 Mrd Dollar umgesetzt, so ist davon auszugehen das einerseits aufgrund einer demographischen andererseits einer technischen Entwicklung dieser weiter am Wachsen ist.

Das WallStreet Journal beschreibt 2011 die elf häufigsten IMGs. (Baxter, 2011)

Einschränkend auf implantierbare Geräte (IMG) sind Gerätekategorien wie Herzschrittmacher, Defibrilatoren, Insulinpumpen und Neurostimulatoren in dieser Arbeit von Bedeutung da diese drahtlose Kommunikation unterstützen. (Gollakota, Hassanieh, Ransford, Katabi & Fu, 2011)

6 Klassifizierung

Bestehende Sicherheitsklassifikationen der Biomedizinischen Technik, der Medizin oder der Informationssicherheit lassen sich nur teilweise auf die Schutzklassifizierung von IMGs an-

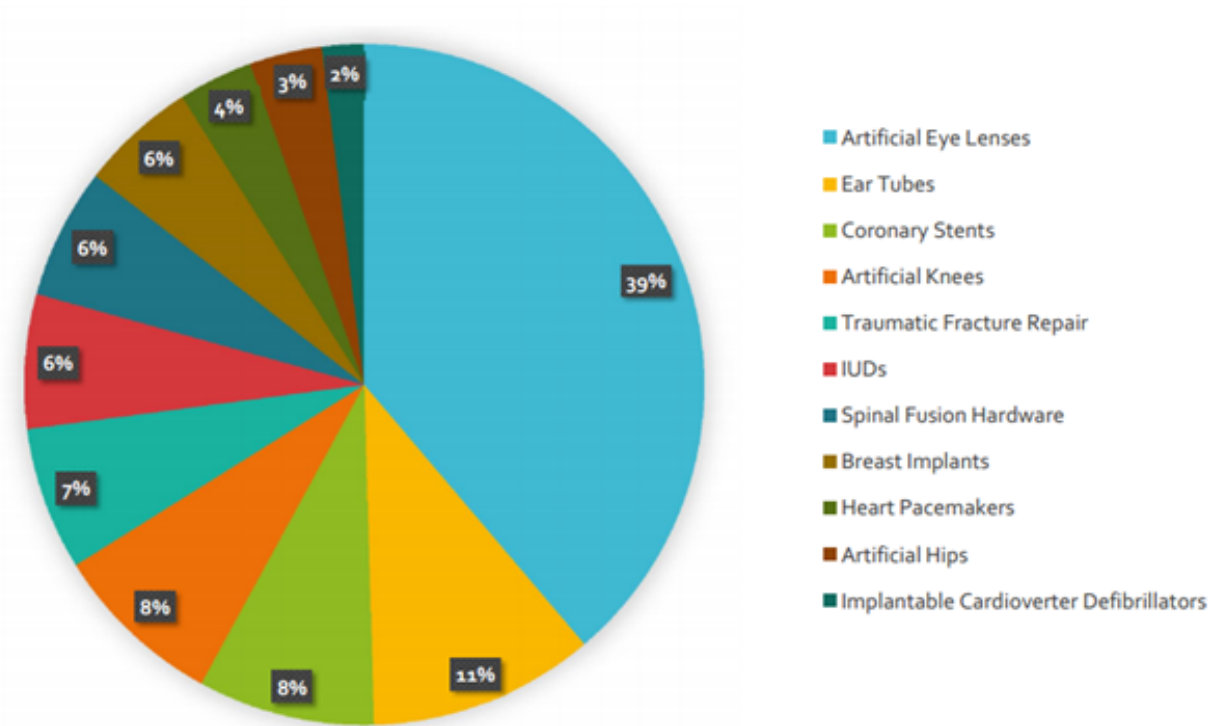


Abb. 2. The Eleven Most Implanted Medical Devices In America in 2011 (Baxter, 2011)

wenden. Sie sind einzeln betrachtet zu restriktiv um direkt zur Entwicklung von IMG Sicherheitsmodellen verwendbar zu sein. Hansen und Hansen (2010) entwickeln in ihrem Artikel durch das Verbinden mehrerer Sicherheitsklassifikationen ein 'Big Picture' um sicherheitsrelevante Verwundbarkeiten und infolge Gegenmaßnahmen zu entwerfen. (Hansen & Hansen, 2010)

6.1 Biomedizinische Technik

Speziell in europäischen Ländern müssen Hersteller von IMGs hohen Standards beim Entwerfen und Testen ihrer medizinischen Produkten entsprechen. Das 'National Research Ethics Service' in den UK klassifiziert folgende schwerwiegende unerwünschte Ereignisse, welche auftreten können:

- Resultiert in Tod

- Lebensbedrohend
- Resultiert in Krankenhausaufenthalt bzw. Verlängerung dessen
- Resultiert in Behinderung bzw. Einschränkung
- Ruft eine kongenitale Anomalie oder einen Geburtsfehler hervor
- Ist auf eine andere Art medizinisch signifikant negativ

Hansen und Hansen (2010) verwenden diese Klassifizierung um die Effekte von IMG Manipulation zu definieren.

6.2 Medizin

Die ICD-10 (International Statistical Classification of Diseases and Related Health Problems) sehen vier Kategorien für Komplikationen von IMGs vor:

- **T82:** Komplikationen von Herz und Gefäß Implantaten
- **T83:** Komplikationen von urogenitalen Implantaten
- **T84:** Komplikationen von internen orthopädischen Implantaten
- **T85:** Komplikationen von innenliegenden Implantaten

(Hansen & Hansen, 2010)

6.3 Informationssicherheit

Relevante Klassifikationen im Feld der Informationssicherheit werden grundsätzlich in zwei Gruppen aufgeteilt:

- Bedrohungen des Systems
- Evaluierung der Verwundbarkeit

Hansen und Hansen (2010) lehnen sich an diese an und entwickeln daraus ihre Risikoklassifikation für IMGs beziehungsweise deren Verwendung.

6.4 Klassifikation der Auswirkungen

Die Kombination der medizinischen Klassifikationen der Komplikationen mit den schwerwiegenden unerwünschten Ereignissen der biomedizinischen Technik lassen Hansen und Hansen (2010) zu zwei Kategorien kommen:

- IMG Aktivität
- Schwerwiegende Effekte

Vergleiche Abbildung 3 für eine tabellarische Gegenüberstellung der beiden Kategorien.

Device	Adverse Events
Pacemaker, implanted cardiac defibrillator [27], ventricular assist device [15]	Heart failure, tachycardia, bradycardia, arrhythmia
Cochlear implant	Deafness, phantom sounds, distraction/confusion
Prosthetic limb control system [38]	Injury, damage to prosthetic limb, inadvertent movement
Spinal cord stimulator [29]	Loss of pain relief, inappropriate stimulation
Sacral anterior root stimulator [8]	Infection from inability to void, inappropriate stimulation
Retinal prosthesis [10], implanted contact lens, intraocular lens	Blindness, phantom images, distraction/confusion
Implanted infusion pump	Inappropriate dosage/timing
Brain-machine interface, other neuroprosthesis [32, 34]	Loss of consciousness, neural effects [14]
Responsive neurostimulator, other deep brain stimulator [35]	Inappropriate stimulation, failure to stimulate
Implanted monitor or sensor	Incorrect readings
Implanted RFID tag [17]	Loss of privacy, data leakage
Implanted dynamic LED tattoo	Inappropriate display

Abb. 3. Potentielle schwerwiegende Folgen in IMGs (Hansen & Hansen, 2010)

6.5 Klassifikation der Verwundbarkeit

Die Vulnerabilität von IMGs hängt laut Hansen und Hansen (2010) im Wesentlichen von zwei verschiedenen Kategorien ab: Der Nähe vom Angreifer zum zu manipulierenden Geräte und von der Funktion des Gerätes an sich.

Physische Nähe: Zeitlich langanhaltender, direkter physischer Kontakt eines Angreifers zu einem willigen oder bewusstlosen Patienten macht praktisch nahezu alle IMGs offen für

Angriffe. Hansen und Hansen (2010) lassen in ihrer Arbeit jedoch diese Fälle konkret aus, da sie sich auf vom Patienten unbemerkte Angriffe festlegen. Sie definieren folgende physischen Näheverhältnisse zwischen Angreifer und Patient:

- Kontakt: Berührung
- Kurz: bis zu 1 Meter
- Medium: 1 Meter bis 50 Meter
- Weit: Über 50 Meter
- Sichtkontakt
- Netzwerk

Funktion: Die Funktion des IMGs beeinflusst direkt sowohl die Vulnerabilität gegenüber unbefugte Veränderungen wie auch die Effekte welche daraus entstehen. Hansen und Hansen (2010) unterteilen in folgende vier Funktionsweisen von IMGs:

- Messend: Informationen vom Patienten oder seiner Umgebung sammeln
- Wirkend: Erwirkt einen Effekt, normalerweise therapeutischer Natur
- Informationsverarbeitend: Aggregiert oder berechnet Informationen
- Kommunizierend: Kontakt mit anderen IMGs, externen Geräten oder dem Patienten

6.6 Folgen

Die schwerwiegenden Folgen, wie in Abschnitt 6.4 angesprochen werden von Hansen und Hansen (2010) anhand zweier Merkmale klassifiziert. Einerseits welche Komponenten betroffen sind und andererseits die Dauerhaftigkeit der Folgen.

Betroffene Komponenten: Betroffen sein können neben dem manipulierten Gerät ebenfalls in Kommunikationskontakt stehende Geräte sein. Diese können neben anderen IMGs externe Geräte wie Computer oder Anzeigen und Displays sein. Im schlimmsten Fall betrifft

es jedoch auch den Patienten selbst. Somit kann der Angriff direkte und indirekte Auswirkungen hervorrufen. (Hansen & Hansen, 2010)

Dauerhaftigkeit: Wenn der Effekt des Angriffs nach einiger Zeit wieder nachlässt und verschwindet oder nur solange anhält, solange der Angriff besteht sprechen Hansen und Hansen (2010) von einer temporären Dauerhaftigkeit. Wird jedoch die Software beziehungsweise die Firmware des IMGs verändert sprechen die beiden Autoren von einer persistenten Dauerhaftigkeit. Der schlimmste Fall, der Tod des Patienten, fällt ebenfalls in diese Kategorie.

Threat	Proximity	Activity	Patient State	Component(s) Affected	Permanence
Headphones with magnetic interference [24]	Contact	N/A	N/A	Target IMD (Actuating), Patient (Heart)	Temporary
Plastic slide [31]	Contact	N/A	N/A	Target IMD (Actuating), Patient (Hearing)	Temporary
Wireless traffic sniffing	Medium	Communicating	N/A	Target IMD (Communicating)	Temporary
Wireless pacemaker exploit [halperin:pacemakerexploit]	Short	Communicating	N/A	Target IMD (Actuating), Patient (Heart)	Temporary
Contrived ILT exploit (see §3.5)	Network	Communicating	Glucose level	External device	Temporary
Contrived prosthetic eye exploit (see §3.5)	Line of sight	Actuating	Visual pattern	Target IMD (Actuating)	Permanent

Abb. 4. Eine Übersicht über mehrere Verwundbarkeiten anhand der Klassifikation von Hansen und Hansen (2010)

7 Sicherheitsmaßnahmen, Vorkehrungen und Verteidigungsstrategien

Einerseits sind es vorbeugende Maßnahmen welche Risiken verhindern oder zu mindestens vermindern sollen und andererseits Maßnahmen welche bei Angriffen oder Schadenseintritt die damit einhergehenden Auswirkungen möglichst gering halten.

7.1 Präventive Maßnahmen

Staatliche als auch supranationale Organisationen wie die Europäische Union stellen grundsätzliche Richtlinien für IMG's und den Umgang mit diesen zur Verfügung.

Hinsichtlich Medical Devices existiert von der FDA (Amerikanischen Gesundheitsbehörde) einerseits ein Leitfaden für Medical Device Security andererseits eine Erfahrungsdatenbank MAUDE (Manufacturer and User Facility Device Experience Database) welche Usererfahrungen aufzeichnet über Medizinische Geräte hinsichtlich IT Sicherheitsrelevanter Belange. (FDA, 2014)

Auf europäischer Seite existiert die Richtlinie 90/384/EWG des Rates vom 20. Juni 1990 zur Harmonisierung der Rechtsvorschriften für implantierbare medizinische Geräte. Die letztgültige Änderung beziehungsweise Berichtigung dieser Richtlinie bezogen auf Anwendung beim Menschen ist aktuell in der Richtlinie 2007/47/EG festgehalten. (EU, 2012)

Aktuell existieren mehrerer Frameworks durch welche einerseits bisherige Ziele wie vernünftige Brauchbarkeit und Betriebssicherheit als auch Security und Privacy bei IMG's erreicht werden soll. Halperin et al. (2008) stellt ein derartiges Framework vor mit welchem Sicherheit und Privatsphäre der Daten zukünftiger IMG's evaluiert werden soll. Die Schwierigkeit besteht darin eine Balance zwischen den genannten Zielen zu finden. Um Kommunikation mit IMG über größere Distanzen zu ermöglichen stellen Gollakota et al. (2011) einen weiteren Lösungsansatz vor, welcher

7.2 Aspekte der Betriebssicherheit und Anwendbarkeit

Der Zugriff auf Daten muss durch berichtigte Geräte gegeben sein da diese Daten in normalen oder Notfallsituation sehr relevant sein können. Wie in Abbildung 2 am Beispiel eines Defibrillators dargestellt ergeben sich technische Anforderungen an das Gerät selbst, an die drahtlose Kommunikation und an Ausfallsicherheit des gesamten Systems.

Um Betriebssicherheit und Anwendbarkeit zu erwirken sind nach Halperin et al. (2008) folgende Kriterien ausschlaggebend: Der Zugriff auf Daten (Data access) muss für autorisierte Geräte oder Individuen bei Bedarf möglich sein. Diesbezüglich sind jegliche Daten in Verbindung mit einem IMG von Belangen. Die gemessenen und gespeicherten Daten sollten adäquat den Anforderungen an ein System hinsichtlich ihrer Datengenauigkeit genügen. Dies kann auch für Zeitliche Daten gelten.

Die Geräte Identifikation ist wesentlich das beispielsweise bei einer Operation ein Gerät identifiziert werden muss und autorisierten Teilnehmern Rechte und Informationen eingeräumt sein müssen. Folglich gilt dies auch für eine notwendige Konfigurierbarkeit und eine Updatebarkeit der Software. Sollten Patienten mehrere IMG tragen oder mehrere IMG in Kommunikationreichweite beispielsweise eines Programmes sein so ist es von Nöten das die Koordination zwischen den Geräten gewährleistet ist. Dies ist auch unter dem Begriff Multidevice coordination zusammengefasst. Um sicherzustellen das jegliche Fehler bei Geräten erkannt werden können sind Prinzipien der Auditierbarkeit notwendigerweise zu berücksichtigen. Ressourceneffizienz ist wesentlich um eine maximale Lebenszeit eines Gerätes einerseits hinsichtlich des Auskommens mit gespeicherter Energie andererseits bezüglich des maximalen Verfügbarkeitszeitraums selbst.

7.3 Aspekte zu Maßnahmen zur Erreichung von Sicherheitszielen und Privatsphäre

Nach Halperin et al. (2008) sind folgende Kriterien hinsichtlich Ziele der Sicherheit und Privatsphäre ausschlaggebend:

Autorisierung von Personal das nur bestimmte Individuen ihnen zugestandene Anwendungen durchführen können. Weiter verfeinert ist dies auch durch ein Rollenkonzept werden indem Autorisierte Individuen Zugriff durch eine zugewiesene Rolle erhalten. Unterschiedliche Rollen

nehmen dabei beispielsweise der Patient selbst, der Mediziner, der Ambulanz Computer oder der Geräte Hersteller ein.

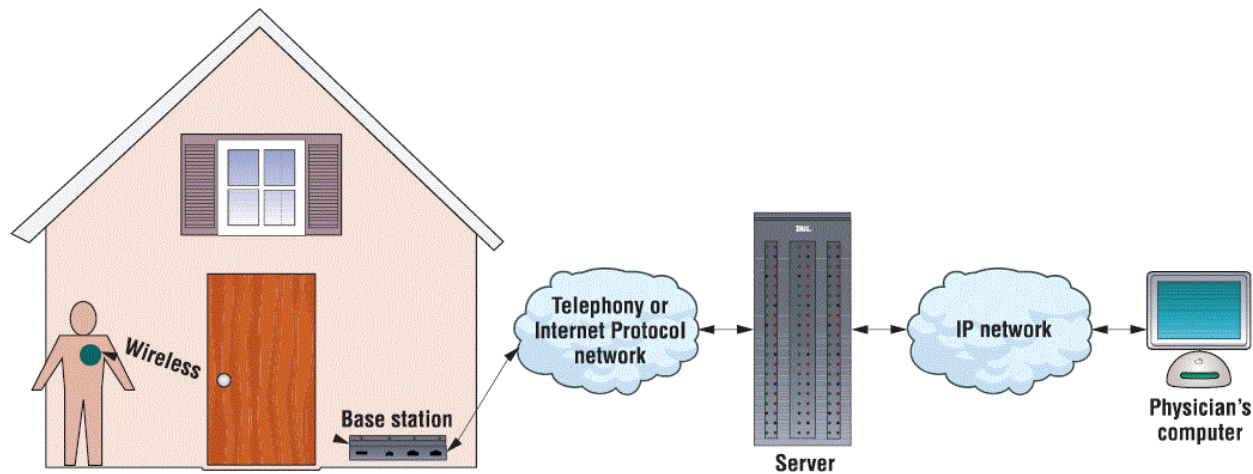


Abb. 5. Defibrillator mit Home Monitoring durch Webzugriff

Kommuniziert ein Gerät mit mehreren IMGs so muss sichergestellt werden dass die Kommunikation nur mit dem beabsichtigten Gerät statt findet. Diese wird wiederum durch Autorisierungs- und Authentifizierungsmaßnahmen erreicht. Als Zugriffsmodell könnte eine von Gupta, Mukherjee und Venkatasubramanian (2006) vorgestellte Lösung zum Einsatz kommen. Des weiteren stellt die Verfügbarkeit einen (lebens-) wichtigen Punkt dar, gerade wenn es Denial of Service Angriffe geht. Die Gerätesoftware muss ausreichend zuverlässig in Hinblick auf Implementierungs- und Entwicklungsfehler sein. Ausreichende Abhilfe muss durch Softwaretests seitens des Hersteller geschaffen werden. Ein fehlerhaftes Verhalten eines Herzschrittmachers kann beispielsweise gravierende Auswirkungen für einen Patienten haben.

Device existence privacy beschreibt dass das IMG nicht für andere unautorisierte Geräte sichtbar ist. Sollte trotzdem Sichtbarkeit gegeben sein ist sicherzustellen dass die Type des Geräts (Device type privacy) und die Geräte ID (Specific device ID privacy) nicht verraten werden, um einen möglichen Angriff zu unterbinden. Weiters sind Messdaten und Logs dieser

unautorisierten Personen vorzuenthalten. Es soll auch nicht möglich sein, sollte das Gerät erkannt werden über einen Exploit den Träger des Gerätes zu identifizieren. Dies wird als Bearer Privacy bezeichnet. Schlussendlich muss auch die Daten Integrität jeglicher Daten welche mit dem Patienten und dem IMG in Verbindung stehen gewahrt bleiben. Eine mögliche Manipulation beispielsweise von Logdaten könnte zu einem falschen Setting des Gerätes führen und dies dem Träger schaden. (Halperin et al., 2008)

7.4 Aspekte der Kommunikation

Ein Kommunikationskanal eines IMG's zu einem Personal Computer oder einem Smartphone bringt zwar die Vorteile eines Datenaustausches mit sich, dadurch entsteht jedoch auch ein möglicher Angriffspfad. Abhilfe könnte dadurch geschaffen werden das ein IMG unterschiedliche Schnittstellen für die unterschiedlichen Geräte mit welchen er kommuniziert anbietet. Dabei kann die Art der Verbindung ob bidirektional oder unidirektional (nur senden oder nur empfangen) einen entscheidenden Beitrag zur Betriebssicherheit leisten. Die meisten IMGs unterstützen nur eine Kommunikation mit Abständen von 2 bis 5 Zentimetern. Den Forschern der Oak Ridge Nationale Laboratory (ORNL) ist es jedoch gelungen mit IMGs über 30 Meter zu kommunizieren. (Leavitt, 2010)

Eine weitere Absicherung der Kommunikation kann durch Verschlüsselung erreicht werden. Dies bringt jedoch den Nachteil mit sich das Verschlüsselung Rechenleistung und einen damit einhergehenden Energieverbrauch den Geräten abfordert. Begrenzte Akkukapazitäten limitieren den Einsatz von kryptographischen Verfahren. Alternativ stellen Halperin et al. (2008) ein System Namens Zero Power Defense vor, welches der IMG von außen mit ausreichend Energie für Kryptographische Anwendungen gespeist wird. Diese Energie kann aus der Sendeleistung des Gateways bezogen werden.

Um den Zugriff auf IMGs zu erschweren könnten Passwortabfragen eingesetzt werden, was jedoch nicht bestimmte Problem mit sich bringt. Probleme beispielsweise dahingehend das bei Notfällen ein Arzt das Passwort nicht kennt. Abhilfe könnte durch Tätowierung dieses geschaffen werden, wobei dabei vermutlich nicht die Zustimmung aller betroffenen IMG Träger erfolgen würde. Alternativ könnten auch Ketten mit oder Armbänder bei denen das benötigte Passwort hinterlegt wird verwendet werden. (Leavitt, 2010)

Gollakota et al. (2011) schlägt hinsichtlich Kommunikation ein Design vor welches „The Shield“ genannt wird. Das Schild wirkt einerseits gegen passives Abhören indem aus dem Jamming Signal und dem Antidote Signal wie in Abbildung 7 dargestellt verschleiert Daten übertragen werden und in anderer Hinsicht gegen aktive Kommunikation mit unautorisierten Signalen indem zwischen dem Schild und dem Programmer, wie in Abbildung 6 dargestellt Daten nur verschlüsselt übertragen werden. Würde ein Angreifer Daten zum IMG übertragen erkennt dies das Shield und unterbindet durch das aktivieren des Jamming Signals die Kommunikation. Um Angriffe zu erkennen findet ein permanentes Lauschen seitens des Schildes statt. Ein wesentlicher Grund die Schild Technologie zu verwenden kann darin bestehen das die Kommunikationsdistanz zwischen dem Programmer und dem IMG wesentlich erweitert und folglich sogar eine permanente Kommunikation unter bestimmten Vorraussetzungen über das Internet ermöglicht wird.

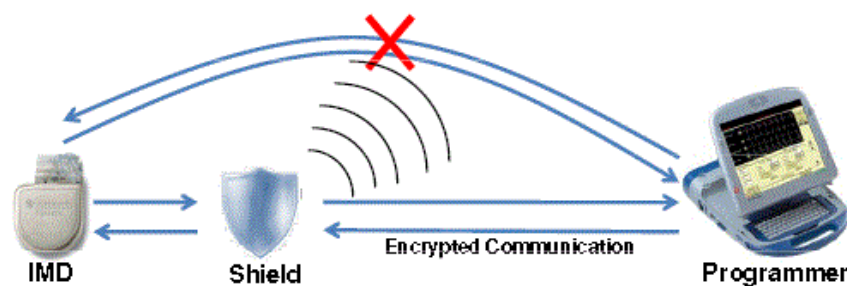


Abb. 6. Schutz der Kommunikation zwischen Programmer und IMG durch das Shield (Gollakota et al., 2011)

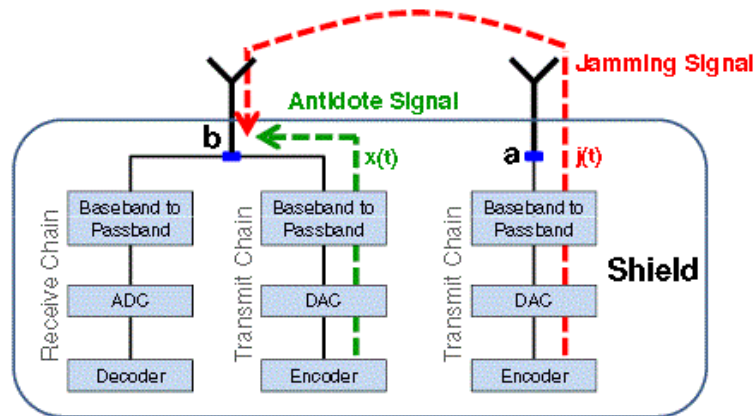


Abb. 7. Kommunikationsdesign innerhalb des Shields (Gollakota et al., 2011)

8 Fazit, Zusammenfassung und Ausblick

Im medizinischen Bereich nehmen die Sicherheit und Privatsphäre von Patienten, sowie die Zuverlässigkeit der Technik einen sehr hohen Stellenwert ein. Da implantierbare medizintechnische Geräte erst innerhalb des letzten Jahrzehnts weite Verbreitung fanden, hat es einen gewissen Zeitraum gedauert bis in diesem Bereich ernstzunehmende Anstrengungen unternommen wurden, die darauf ausgerichtet waren einen hohen Sicherheitsstandard zu gewährleisten.

Herkömmliche Sicherheitstechniken aus dem IT-Bereich können im Kontext von IMGs nur bedingt angewandt werden, da die meisten implantierten Geräte batteriebetrieben sind und somit das Streben nach Energieeffizienz ein konkurrierendes Ziel darstellt, wobei keines der beiden vernachlässigbar werden darf. In Zukunft gilt es schrittweise Optimierungen vorzunehmen und effiziente Methoden miteinander zu kombinieren um den Erreichungsgrad beider Ziele steigern zu können.

Literatur

- Baxter, A. (2011, jul). *The eleven most implanted medical devices in america*. Zugriff auf <http://247wallst.com/healthcare-economy/2011/07/18/the-eleven-most-implanted-medical-devices-in-america/>
- Daniluk, K. & Niewiadomska-Szynkiewicz, E. (2012). Energy-efficient security in implantable medical devices. In *Computer science and information systems (fedcsis), 2012 federated conference on* (S. 773–778).
- EU. (2012, dez). *Richtlinie 2007/47/eg*. Zugriff auf http://europa.eu/legislation_summaries/consumers/consumer_safety/l21010a_de.htm
- FDA. (2014, jun). *Manufacturer and user facility device experience database - (maude)*. Zugriff auf <http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/ReportingAdverseEvents/ucm127891.htm>
- Gollakota, S., Hassanieh, H., Ransford, B., Katabi, D. & Fu, K. (2011). They can hear your heartbeats: non-invasive security for implantable medical devices. *ACM SIGCOMM Computer Communication Review*, 41 (4), 2–13.
- Grimes, S. (2004). Medical device security. In *Engineering in medicine and biology society, 2004. iembs'04. 26th annual international conference of the ieee* (Bd. 2, S. 3512–3514).
- Gupta, S. K., Mukherjee, T. & Venkatasubramanian, K. (2006). Criticality aware access control model for pervasive applications. In *Pervasive computing and communications, 2006. percom 2006. fourth annual ieee international conference on* (S. 5–pp).
- Halperin, D., Heydt-Benjamin, T. S., Ransford, B., Clark, S. S., Defend, B., Morgan, W., ... Maisel, W. H. (2008). Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Security and privacy, 2008. sp 2008. ieee symposium on* (S. 129–142).
- Hansen, J. A. & Hansen, N. M. (2010). A taxonomy of vulnerabilities in implantable medical

devices. In *Proceedings of the second annual workshop on security and privacy in medical and home-care systems* (S. 13–20).

Hosseini-Khayat, S. (2011). A lightweight security protocol for ultra-low power asic implementation for wireless implantable medical devices. In *Medical information & communication technology (ismict), 2011 5th international symposium on* (S. 6–9).

Leavitt, N. (2010). Researchers fight to keep implanted medical devices safe from hackers. *Computer*, 43 (8), 11–14.