Hochschule Reutlingen
Reutlingen University

INF
Informatik

Uwe Kloos, Natividad Martínez, Gabriela Tullius (Hrsg.)

Informatics Inside
connect(IT);

Informatik-Konferenz an der Hochschule Reutlingen
9. Mai 2018

9 783000 586453

Impressum

Anschrift:
Hochschule Reutlingen / Reutlingen University
Fakultät Informatik
Human-Centered Computing
Alteburgstraße 150
D-72762 Reutlingen

Telefon: +49 7121 / 271-4002
Telefax: +49 7121 / 271-4042

E-Mail: infoinside@reutlingen-university.de
Internet: http://infoinside.reutlingen-university.de

Organisationskomitee:
Prof. Dr. Gabriela Tullius, Hochschule Reutlingen
Prof. Dr. Natividad Martínez, Hochschule Reutlingen
Prof. Dr. Uwe Kloos, Hochschule Reutlingen

Benjamin Batt
Claudiu Bräuer
Sinem Cicek Celik
Emanuel Geiger
Frauke Grieble
Peter Grupp
Pia Laubacher
Öznur Öner
Katharina Pavic
Ngoc Linh Phan
Claudia Ryniak
Josia Scheytt
Christian Steinmann
Clemens Weißenberg
Vanessa Willenbrock
Steffen Wittig

Copyright: © Hochschule Reutlingen, Reutlingen 2018
Herstellung und Verlag: Hochschule Reutlingen
ISBN: 9 -83000-586453

Inhaltsverzeichnis

Longpaper

Untersuchung der Möglichkeiten und Risiken von Implantaten

Benjamin Weinert
Reutlingen University
Benjamin.Weinert@Student.
Reutlingen-University.DE

Abstract
Durch das stetige Wachstum an neuen Technologien und Möglichkeiten steht der Verschmelzung von Technologien mit dem Menschen kaum noch etwas im Wege. Die Untersuchung der Implantate und die damit verbundenen Risiken sind ein Teil dieser Arbeit. Von Bedeutung sind hier die Funktionsweise und die IT-Sicherheitsaspekte. Alle in dieser Arbeit dargestellten Implantate benötigen eine Kommunikation nach außen. Diese Kommunikationsmöglichkeit birgt Risiken, die nicht nur auf die Daten der Träger beschränkt sind, sondern auch gesundheitliche Risiken beinhalten.

Schlüsselwörter
RFID, Retina, Sicherheit, Implantat, Mikrochip, Hacking, Risks, Medizin, Biohacking, Hardware

CR-Kategorien
Security, Human Factors, Design, Algorithms, Hardware

Betreuer Hochschule: Prof. Dr. Tangemann
Hochschule Reutlingen
Michael.Tangemann@Reutlingen-University.de

Informatics Inside 2018
Wissenschaftliche Vertiefungskonferenz
09. Mai 2018, Hochschule Reutlingen
Copyright 2018 Benjamin Weinert

1 Einleitung
Die immer kleiner werdenden Technologien finden nicht nur in Computersystemen ihre Anwendung, sondern sie bestimmen schon heute den Alltag der Menschen. Mikrochips werden für das Bezahlen mit der EC-Karte, für Zugangsberechtigungen anhand von Zugangskarten und für medizinische Anwendungen wie Herzschrittmacher verwendet. Das neueste Anwendungsgebiet stellen jedoch Implantate dar. In Filmen wie „The Circle“ oder „Ghost in the Shell“ werden fiktive Implantate dargestellt, die der körperlichen Gesundheitsüberwachung oder als Upgrades für menschliche Fähigkeiten dienen.

Neben den unterschiedlichen Einsatzgebieten der Mikrochips, wie beispielsweise in der Medizin oder der Vernetzung des Menschen, werden Mikrochips auch für die Wireless-Übertragung von Daten verwendet. Dies bedeutet, es muss eine Kommunikationsmöglichkeit integriert sein, welche zusätzlich an der Energieversorgung angeschlossen ist und somit den Energieverbrauch erhöht.

Die Übertragung von Daten über die Luft birgt zudem ein gewisses Risiko. Böswillige Zugriffe auf diese Mikrosysteme können erheblichen Schaden anrichten, nicht nur datenschutztechnischen durch das Stehlen von privaten Informationen, sondern in diesem Falle auch gesundheitlichen. Gelingt es jemanden diese Datenübertragung abzufangen und direkten Zugriff auf die

Daten zu erhalten, besitzt er die Möglichkeit diese für weitere Angriffe zu verwenden.

1.1 Ziel und Aufbau

Ziel der Arbeit ist es zunächst, einen Überblick über die untersuchten Implantate zu geben. Die Auswahl der Implantate wurde so gewählt, dass ein bereits seit längerem bestehendes, ein neueres und ein sich noch in der Forschung befindliches untersucht wird. Des Weiteren wird anschließend auf die IT-sicherheitsspezifischen Fragen eingegangen und die Implantate auf mögliche Angriffe untersucht. Hierzu werden bereits bekannte Angriffsmöglichkeiten auf die Technologien berücksichtigt und neue Angriffsvektoren aufgedeckt, die sich durch die Anwendung von Implantaten ergeben. Dabei werden nicht nur technische Angriffe berücksichtigt, sondern auch gesundheitlich relevante Punkte angesprochen.

Die Arbeit gliedert sich somit in zwei Hauptteile, zum einen die Vorstellung der Implantate und zum anderen die Untersuchung der Implantate in Hinsicht auf die IT-Sicherheit und die gesundheitlichen Risiken. Die in den nachfolgenden drei Kapiteln vorgestellten Implantate besitzen zudem eine kabellose Kommunikationsschnittstelle, welche für die IT-Sicherheit eine relevante Eigenschaft darstellt.

2 Herzschrittmacher

Die Definition von Implantaten ist laut [1] wie folgt. Implantate sind künstliche Teile zur Erfüllung bestimmter Ersatzfunktionen, die in den menschlichen Körper eingebracht werden. Der Herzschrittmacher wie er verallgemeinert genannt wird, ist eines der bekanntesten Implantate. Herzschrittmacher und Defibrillatoren werden umgangssprachlich nicht unterschieden, jedoch führen beide unterschiedliche Funktionen aus. Defibrillatoren springen nur ein, wenn zum Beispiel ein Kammerflimmern erkannt wird und versuchen das Herz wieder in den normalen Sinusrhythmus zu bringen. Der Herzschrittmacher hingegen wird zum kardinalen Rhythmusmanagement eingesetzt. Dieser greift nur bei Pausen oder zu langsamer Aktivität des Herzens ein, dabei überwacht der Herzschrittmacher permanent die Herzaktivität.

Ein Herzschrittmacher ist im Wesentlichen ein batteriebetriebener Impulsgenerator, welcher bei bestimmten Herzrhythmusstörungen durch elektrische Stimulation des Herzens für einen normalen Herzrhythmus sorgt [2]. Das etwa streichholzschachtelgroße Gehäuse beinhaltet die Stimulator- und Analyseelektronik sowie die Batterie [2]. Eingesetzt wird es normalerweise unter dem Schlüsselbein unter örtlicher Betäubung [2]. Bis zu drei ca. 60cm lange Elektroden werden zum Herzen vorgeschoben und am Herzmuskel befestigt [2].

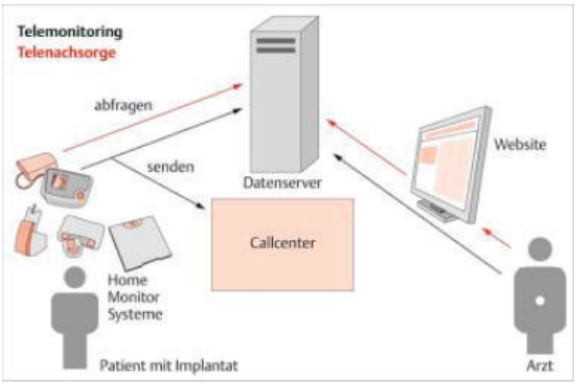

Abbildung 1: Telemonitoring und Telenachsorge [3]

Aktuelle Generationen von Herzschrittmachern besitzen eine Kommunikationsschnittstelle nach außen [3]. Diese wird dazu verwendet, Nachsorgetermine zu reduzieren und die Überwachung durch den Arzt auch dann zu ermöglichen, wenn dieser nicht direkt vor Ort ist. Diese Art der Nachsorge nennt man Telenachsorge oder Telemonitoring. Die Telenachsorge bietet hierbei keine kontinuierliche Datenübertragung, sondern ein kontrollierter Datenaustausch zwischen Arzt und Patient. Der Patient hat somit die Möglichkeit gezielt Daten an den Datenserver zu senden, womit der Arzt diese jederzeit abrufen kann.

Das Telemonitoring hingegen bedeutet eine kontinuierliche Datenübertragung vom

Patienten zum Datenserver, wobei der Arzt all diese Informationen live auf dem Monitor verfolgen kann. Die entstehende Datenflut würde bei der Beurteilung durch den Arzt zusätzlichen Zeitaufwand bedeuten, sodass hier Auswertezentren zur Filterung der Daten erforderlich sind [3].

Die Abbildung 1, stellt diese zwei Verfahren dar. Zu erkennen ist, dass für die Übertragung der Daten des Herzschrittmachers ein Home Monitor System benötigt wird. Beim Telemonitoring ist der Ablauf wie folgt: Der Patient überträgt die Daten des Herzschrittmachers an den Datenserver und zeitgleich eine Benachrichtigung an das Callcenter. Der Arzt kann dann die Daten von dem Datenserver abrufen und erhält somit den kontinuierlichen Datenfluss. Bei der Telenachsorge sendet der Patient eine Abfrage an den Datenserver, bevor die Daten des Patienten an den Datenserver gesendet werden. Der Arzt kann dann über eine Website die auf dem Server liegenden Daten des Patienten direkt abrufen. Er erhält dadurch einen Überblick über den Zustand des Herzschrittmachers und die Aktivitäten des Herzens.

3 RFID und NFC Implantat

Ein RFID (Radio Frequency Identification) Implantat ist keine Zukunftsvision mehr, sondern schon Realität, dies zeigt ein Bericht von [4], bei dem sich eine Person selbst RFID-Implantate gesetzt hat. Weitere Beispiele stellen eine US-Firma und eine schwedische Firma dar, die den Mitarbeitern NFC (Near Field Communication) Implantate einsetzen ließen. [5][6]

In der Literatur wird nur spärlich zwischen RFID und NFC unterschieden, daher wird in dieser Arbeit nur RFID verwendet. Beim RFID-Implantat handelt es sich um eine kleine Kapsel. Diese ist nicht größer als ein Reiskorn, jedoch ausgestattet mit einem technischen Innenleben und der Möglichkeit Daten zu übertragen. Die Bauteile ähneln dem normalen Aufbau der RFID-Chips, sie besitzen eine Glaskapsel mit den Maßen 12mm und einen Durchmesser von 2mm. Versorgt wird das Implantat über die Induktion. Dabei erzeugt das Lesegerät ein Magnetfeld, welches von der Antenne genutzt wird.

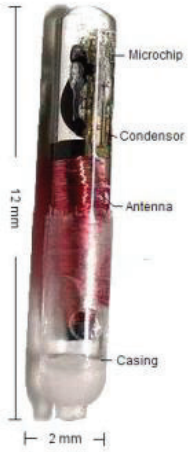

Abbildung 2: RFID-Chipkapsel [7]

Der VeriChip war 2011 der erste RFID-Chip, der für die Implantation im Menschen zugelassen wurde. Auf dem Chip wurden keine persönlichen Daten gespeichert. Auf dem Lesegerät wird lediglich eine 16-stellige Identifikationsnummer abgelesen, welche zu einem Eintrag in der Datenbank führt. Der Eintrag der Datenbank umfasste dabei Angaben über den Implantat-Träger, dessen Ansprechpartner, sowie Informationen über Allergien, Medikation, andere Implantate und frühere chirurgische Eingriffe. [7]

Die RFID-Implantate heutzutage beinhalten dabei sehr viel mehr, als nur eine 16-stellige Identifikationsnummer. Sie sind dazu in der Lage, als Zugangsberechtigung zu fungieren oder persönliche Informationen abzuspeichern. Aktuelle Implantate können auch als Bezahlmöglichkeit verwendet werden; dies hat Graafstra [4] in seinem Selbstversuch bereits bewiesen und zeigt auf, dass noch viel mehr möglich ist. Die RFID-Implantate werden als Rohlinge verkauft und können vom Anwender auch selbst programmiert werden. Dies vergrößert das Einsatzgebiet deutlich und lässt Entwicklern freie Hand, wozu diese die Implantate verwenden [4].

4 Retina Implantat

Ein Implantat oder eine Prothese bezeichnet in der Medizin allgemein den Ersatz von Organen oder deren Teilen [8]. Bezieht man diese Aussage auf das menschliche Auge bedeutet dies, dass ein Teil und dessen Funktion von einem Implantat entweder ganz oder zum Teil übernommen wird. Bei dem Begriff Retina-Implantat geht man jedoch noch einen Schritt weiter und bezieht dies auf solche Technologien, die das Ziel haben, neuronale Funktionen des Sehens zu ersetzen [9].

Innerhalb eines vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projektes wird der Ansatz untersucht, mit Hilfe einer Telemetrie-Anwendung Daten und Energie in das menschliche Auge zu übertragen. Hintergrund ist hierzu die Erkrankung der menschlichen Netzhaut die bei rund 30.000 Menschen allein in Deutschland diagnostiziert wurde. Diese Erkrankung gilt als unheilbar, wie Retinitis Pigmentosa oder Makula-Degeneration. [10]

Es existieren momentan zwei Versionen des Retina-Implantats. Zum einen das subretinale Implantat und zum anderen das epiretinale Implantat, welche sich nicht nur in der Funktion unterscheiden, sondern auch im technischen Aufbau.

4.1 Subretinales Implantat

Elektronische Sehimplantate gehören in den Bereich der Neuroprothetik und versuchen Teilfunktionen der neuronalen visuellen Sehbahn zu ersetzen [9]. Das subretinale Implantat ersetzt dabei die Funktion der degenerierten Photorezeptoren – dieser Ansatz wird aktuell in einer klinischen Studie in Tübingen verfolgt [9].

Die Ersetzung erfolgt durch das Implantieren eines Mikrochips, der aus mehreren Bauteilen besteht, wie in der Abbildung 3 zu sehen ist. Das Implantat besteht dabei aus einem Mikrochip Alpha IMS von der Retina Implantat AG, dieser besteht aus 1500 Elementen, die auf einer Fläche von 3 x 3mm platziert sind. Jedes dieser Pixel besteht dabei aus einer lichtempfindlichen Photodiode, einem Differenzverstärker und einer Elektrode. [9]

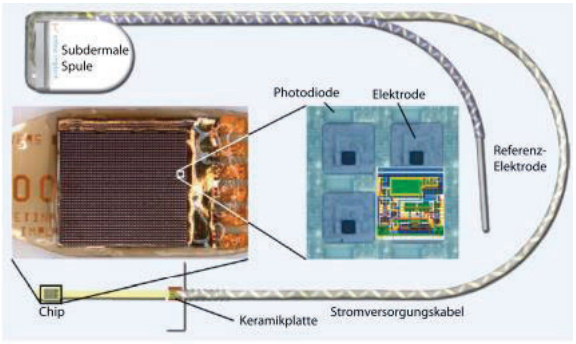

Abbildung 3: Aufbau - Subretinales Implantat [9]

Einfallendes Licht wird Punkt für Punkt von Photodioden aufgefangen und in elektronische Signale umgewandelt, die weiter an den Sehnerv geleitet werden[8].

Die Stromversorgung des subretinalen Implantats wird durch eine externe Stromquelle sichergestellt. Grund hierfür ist die Tatsache, dass das einfallende Licht nicht ausreicht, um den Energiebedarf des Implantats zu decken. Diese externe Stromzufuhr ist auf der Abbildung 3 zu sehen; das Kabel verlässt nach einer als dünne Folie ausgebildeten subretinalen Strecke den Bulbus transchorioidal und transskleral. Es verläuft weiter unter dem Musculus temporalis bis hinter das Ohr und mündet in eine subperiostale Empfangsspule für die Stromversorgung und die Steuersignale. [9]

4.2 Epiretinales Implantat

Im Gegensatz zu dem subretinalen Implantat benötigt das epiretinale Implantat eine externe Kamera, die häufig an Brillen befestigt ist. Dies hat mit der Implantierungsmethode zu tun, denn anders als bei der subretinalen Implantation, wird das Implantat nicht hinter die intakte Netzhaut implantiert, sondern auf die Netzhaut. Die Elektroden stimulieren direkt Ganglienzellen des Sehnervs und

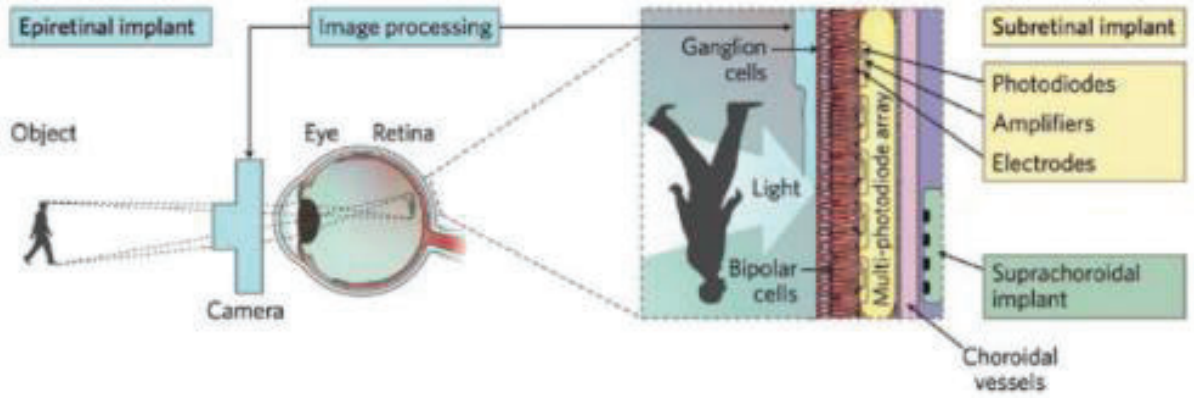

Abbildung 4:Epiretinales (Argus II) und subretinales Implantat (Aplha IMS)[12]

überbrücken somit die gesamte Retina. Generell gilt dieser Eingriff als chirurgisch einfacher zugänglich [11]. Aktuell gibt es zwei verschiedene Systeme des epiretinalen Implantats. Zum einen das Argus II System und zum anderen das EPIRET3 System. Beide Ausführungen verwenden eine außen angebrachte Kamera, die in eine Brille eingelassen wird, und ein Computersystem für die Verarbeitung der Kameradaten.

Das EPIRET3 System [11] besteht dabei aus zwei Teilsystemen, zum einen das extraokulare und zum anderen dem intraokularen. Das extraokulare Teilsystem umfasst dabei ein Computersystem, eine Sendereinheit und eine an einem Halter angebrachte Senderspule, die vor dem Auge platziert wird. Das intraokulare Teilsystem besteht dabei aus einem Empfänger, der notwendigen Elektronik und aus 25 3D-Simulationselektroden. [11]

Das Argus II System ist dabei gleich aufgebaut, wie das EPIRET3 System, jedoch besitzt das Argus II System 60 Elektroden, die aus dem Kamerabild ein Erregungsmuster auf die Netzhaut übertragen [12].

Die Abbildung 4 zeigt die beiden Retina Implantate; deutlich zu erkennen ist hier die Kameravorrichtung vor dem Auge und die Platzierung des epiretinalen Implantats direkt auf der Netzhaut (linker Teil des Bildes). Das subretinale Implantat ist auf dem Bild im rechten Teil zu finden und ist hinter der Netzhaut platziert.

5 Sicherheitsrisiken der Technologien

Sobald Mikrochips und Datenübertragungen möglich sind, gibt es auch Sicherheitsrisiken und mögliche Angriffe, die zu beachten sind. In diesem Kapitel werden mögliche Schwachstellen und konkrete Sicherheitslücken aufgezeigt und diskutiert. Dabei werden die in den Implantaten verwendeten Technologien einzeln betrachtet. Neben den technischen Risiken, werden zudem auch gesundheitliche Risiken angesprochen – dies hat den Grund, da die Technologien und deren technische Bauteile auch gesundheitliche Risiken bergen.

Angriffe auf Technologien verfolgen meist bestimmte Ziele, sei es das System unbrauchbar zu machen, Daten zu erhalten oder einfach Schaden anzurichten und das System temporär zu blockieren. Um diese Ziele zu erreichen, verwenden die Angreifer verschiedene Methoden, auf welche die vorgestellten Implantate untersucht werden.

5.1 Herzschrittmacher

Herzschrittmacher, die eine Wireless Funktion beinhalten, stellen bei Hackern eine unwiderstehliche Versuchung dar [13]. Eine Gruppe von Wissenschaftlern der Universitäten von Massachusetts und Washington gelang es, das Sicherheitssystem des kombinierten Herzschrittmachers mit dem Defibrillator der Firma Medtronic zu überwinden [13]. Ihnen ist es nicht nur gelungen, persönliche Daten auszulesen, sondern sie wären zu dem in der Lage

gewesen, tödliche Stromstöße an ein normal funktionierendes Herz zu senden [13].

Dem bekannten Hacker Barnaby Jack gelang es, eine Reihe von Geräten aus dem Internet der Dinge zu hacken, von Geldautomaten bis hin zu Herzschrittmachern. 2012 entdeckte Jack ernsthafte Schwachstellen in der Software implantierbarer medizinischer Geräte verschiedener Hersteller und es gelang ihm, diese Geräte selbst zu steuern. Aus einer Entfernung von 15 Metern hätte er allein mit einem Befehl über seinen Laptop einen implantierten Defibrillator anweisen können, Stromstöße von 830V in das Herz eines Betroffenen zu schicken. [13]

Solche Angriffe wären für den Implantatbesitzer tödlich und zeigen auf, welche Gefahren aus der Vernetzung des Menschen hervorgehen. Die Sicherheitslücke der Herzschrittmacher und Defibrillatoren war durch die Software verschuldet, welche anschließend durch ein Firmware-Update geschlossen wurde [13]. Aus diesem Anlass entschied sich der Kardiologe des ehemaligen Vizepräsidenten Dick Cheney bei dessen Herzschrittmacher die Funkfunktion abzuschalten, damit keine Terroristen einen tödlichen Stromstoß an das schon leidende Herz schicken können [13].

Der Hacker Barnaby Jack erläuterte sein spezifisches Vorgehen zwar bestimmten Herstellern und seinem befreundeten Sicherheitsforscher Laverett, jedoch nicht der Öffentlichkeit. Somit bleibt es streng geheim, wie genau es Barnaby Jack geschafft hat, die Implantate durch einen manipulierten Transmitter zu steuern [14].

5.1.1 Gesundheitliche Risiken

Neben dem Risiko eines Angriffes und der dadurch verursachten Schäden am Herzen, besitzen Herzschrittmacher weitere gesundheitliche Risiken, die es zu untersuchen gilt. Herzschrittmacher sind anfällig, wenn starke Magnetfelder in der näheren Umgebung sind. Zwar unterscheiden sich die verschiedenen Generationen von Herzschrittmachern bezüglich der Anfälligkeit, jedoch besitzen nicht alle einen der neuesten Generation. Daher gelten Herzschrittmacher als Kontraindikation für MRT (Magnetresonanztomographie), dies bedeutet, dass bei Patienten die einen Herzschrittmacher besitzen, eher von einem MRT abgesehen werden sollte. [2]

Gesundheitliche Risiken können auch von einem Angriff ausgehen, wie in Kapitel 5.1 beschrieben. Dabei muss ein Angriff nicht unbedingt tödlich enden, sondern kann auch eine Auslastung auslösen, die die verwendete Batterie erschöpft oder das Herz und seinen Rhythmus beeinflusst. Somit wäre es denkbar, dass ein Kammerflimmern oder eine Herzrhythmusstörung ausgelöst werden kann, die die Gesundheit des Patienten gefährdet.

5.2 RFID und NFC Implantat

Die RFID Technologie ist eine ältere Technologie, die in Chip-Karten, wie bei Zugangskarten eingesetzt wird. Bei einem RFID-Implantat bestehen daher auch die schon bekannten Sicherheitsrisiken. Anders als bei Chipkarten, kann der Träger sein Implantat nicht einfach ablegen und trägt es somit immer bei sich. Dies erhöht das Risiko eines Angriffes. Zusätzlich ist der Besitzer dieser RFID Implantate dazu in der Lage, diese selbst zu programmieren, was das Risiko nochmal erhöht, da die gängigen Sicherheitsmechanismen wie beispielsweise kryptografische Verschlüsselung, nicht zwingend bedacht werden.

In den nachfolgenden Unterkapiteln werden Angriffsmöglichkeiten vorgestellt und diskutiert. In Abbildung 5, sind verschiedene Angriffsmöglichkeiten auf RFID Systeme aufgezeigt. Dabei zeigen die grauen Pfeile und somit die einzelnen Angriffsmöglichkeiten direkt auf das betreffende Element des RFID Systems. In dieser Arbeit können nicht alle Angriffsvektoren genau erläutert werden,

daher wurden nur die ausgewählt, die durch das Implantat ein erhöhtes Risiko darstellen.

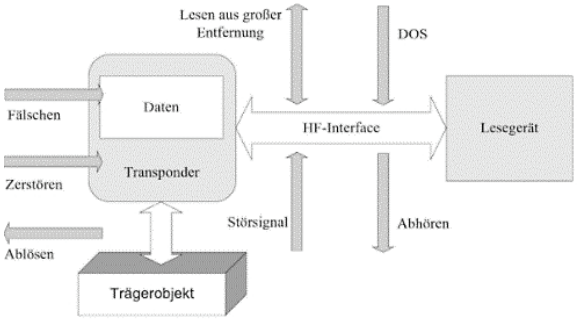

Abbildung 5: Angriffsmöglichkeiten auf RFID Systeme [15]

Somit lassen sich folgende Angriffsmöglichkeiten spezifizieren, welche auch bei einem Implantat angewendet werden können.

5.2.1 Denial of Service

Bei der Zerstörung des RFID-Implantats, können in der Regel zwei Arten angewendet werde. Zum einen die physische Gewalt und zum anderen durch Hilfe von technischen Geräten. In dem Artikel von Graafstra [4] wurde ausprobiert, welche Kraft nötig ist, um das Implantat durch Gewaltanwendung mit einem Hammer zu zerstören. Dabei stellte dieser fest, dass die Gewalteinwirkung so groß sein muss, dass die Hand selbst Schaden erleiden würde.

Die dauerhafte Zerstörung des RFID Implantats kann mittels der Verwendung eines RFID-Zappers erfolgen [16]. Dieser ist ein kleines elektronisches Bauteil, welches ein starkes elektromagnetisches Feld erzeugen kann, ähnlich eines EMP's (elektromagnetischer Impuls) [16]. Dieses Feld erzeugt dabei eine Spannung, welches ein Bauelement der Schaltung des RFID-Chips durchbrennen lassen kann [16]. Im Internet findet man eine Vielzahl von Bauanleitungen, für einen RFID-Zapper [17]. In den meisten Anleitungen werden Bauteile einer Einwegkamera verwendet und eine Art Spule gebaut, siehe Abbildung 6. Jedoch werden bei diesen RFID-Zappern nur von einer Verwendung bei RFID-Chips wie beispielsweise von Personalausweisen berichtet, nicht bei RFID-Implantaten. Somit müsste noch geprüft werden, ob dieses elektromagnetische Feld ausreichend ist, um die Haut und den Glaskörper des Implantats zu durchdringen und so den RFID-Chip zu zerstören. Das Risiko eines solchen Angriffs ist bei einem Implantat größer, da das Implantat immer dabei ist und nicht abgelegt werden kann. Dennoch ist das Implantat von außen nicht leicht zu erkennen, wodurch der Angreifer gezielt wissen muss, dass man solch ein Implantat besitzt. Je mehr die Implantate verbreitet sind, desto größer wird das Risiko eines solchen Angriffs, da der Angreifer davon ausgehen kann, dass man solch ein Implantat besitzt.

Abbildung 6: RFID Zapper, gebaut aus einer Kamera [17]

Neben der Zerstörung des Implantats gibt es noch weitere Möglichkeiten eine Denial of Service Attacke auszuführen. Die einfachste Methode wäre die Kommunikation zwischen Lesegerät und RFID-Implantat zu unterbrechen. Bei RFID-Karten kann dies durch eine einfach metallische Hülle geschehen, jedoch stellt sich dies, bei einem Implantat als schwierig dar. Eine Alternative wäre hier die Verwendung von aktiven Störsendern. Aktive Störsender beeinflussen das elektromagnetische Feld zwischen dem Implantat und dem Lesegerät und unterbrechen die Datenkommunikation [15]. Der Störsender müsste somit, entsprechend nahe am Lesegerät positioniert sein oder mit entsprechend großen Antennen und Sendeleistung gearbeitet werden [15]. Der Schaden, der sich beim Zerstören ergibt, beträgt nur die Kosten des Implantats selbst.

5.2.2 RFID-Malware

Die RFID-Malware ist ein Angriff, der sich nicht nur auf den Transponder oder auf das Lesegerät beschränkt. Die RFID Malware gliedert sich in 3 Kategorien auf. RFID Worms verbreiten sich über ein Netzwerk ohne Benutzeraktivität. Sie führen Aktivitäten wie Löschen von Dateien, Installieren von Software-Patches oder Senden von Informationen per E-Mail durch. Der ganze Worm kann dabei nicht auf dem RFID-Chip platziert werden, daher wird ein Teil auf dem Chip platziert und der Rest wird heruntergeladen. [18]

RFID Viren sind infektiöse RFID Chips, die im Vorfeld manipuliert wurden. Diese Manipulation breitet sich dann über die Lesegeräte bis hin zum zentralen Managementsystem aus und infizieren somit alle RFID Tags oder Implantate die mit diesem System kommuniziert haben. [18]

RFID Exploits können direkt die Backend Middleware nutzen. Für diese Art des Angriffs benötigt es mehr Einfallsreichtum statt Ressourcen. Die Manipulation von den On-Chip-Daten können Sicherheitslücken in der Middleware ausnutzen, wodurch ihre Sicherheit untergraben wird und möglicherweise der gesamte Computer oder das gesamte Netzwerk kompromittiert wird. Je mehr manipulierte Daten auf einen RFID Chip passen, desto komplexere Angriffe können durchgeführt werden. [19]

5.2.3 Klonen des Transponders

Das Klonen oder auch emulieren eines RFID Transponders ist eine komplexere Art des Angriffs. Dabei wird versucht, den RFID Transponder zu kopieren, um somit einen identischen Transponder zu erzeugen. Da die RFID-Implantate auch als Rohlinge gekauft werden können und nicht nur von Firmen verwendet werden, können diese zunächst noch keine Sicherheitsmechanismen vorweisen. Damit besteht die Gefahr, dass das Klonen ohne Hindernisse geschehen kann. Beim Klonen wird versucht die eindeutige ID des RFID Implantats zu kopieren und dessen Speicher, falls vorhanden [15]. Für das Auslesen und Klonen kann ein Aufbau wie in Abbildung 7 gezeigt, verwendet werden.

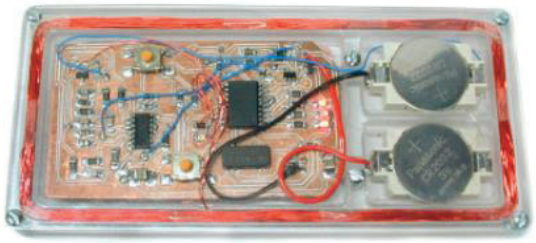

Abbildung 7: Versuchsaufbau zum Auslesen und Klonen eines 125KHz Read-Only Transponders [15]

Der Kopiervorgang geschieht dabei innerhalb weniger Sekunden. Da der Implantat-Träger das RFID-Implantat immer bei sich trägt, kann dieser so gut wie überall ausgelesen werden. Ein Angreifer benötigt hierzu nur ein Lesegerät und ein Laptop, welches sich in einem Rucksack leicht verstauen lässt. Ein wirkungsvoller Schutz gegen das Klonen besteht in der 2 Wege Authentifizierung und der Verschlüsselung [15].

Es ist anzunehmen, dass gerade Firmen die ihren Mitarbeitern RFID-Implantate zur Identifikation anbieten, diese Schutz-mechanismen bereits verwenden. Ein weiterer Schutz ist das Implantat selbst. Das Implantat ist äußerlich nicht bis kaum zu erkennen, somit müsste der Angreifer gezielt wissen, dass eine Person solch ein Implantat besitzt. Hierdurch erhöht sich die Gefahr je mehr Menschen sich ein Implantat einsetzen lassen. Erst wenn diese Praktik zum Alltag der Bevölkerung gehören sollte, kann der Angreifer davon ausgehen, dass es auch ohne eine bestimmte Zielperson, RFID-Implantate zum Auslesen und Klonen gibt.

5.2.4 Gesundheitliche Risiken von RFID-Implantaten

Das RFID-Implantat besitzt nicht nur technologische Risiken, sondern auch gesundheitliche Risiken. Dies wurde von Forschern erstmals bei Tieren festgestellt, die einen Identitätschip implantiert bekamen. Es ist nicht sicher, dass diese gesundheitlichen

Risiken auch beim Menschen auftreten können, da es noch keine Langzeitstudien diesbezüglich gibt. [7]

Es wurden 4 Gründe für die Tumorbildung in Zusammenhang mit implantierten Mikrochips ermittelt [7]. Der erste ist die fremdkörperbedingte Tumorbildung. Da der Mikrochip subkutan implantiert wird und vom Körpergewebe als Fremdkörper betrachtet wird, kann die Kommunikation zwischen den Zellen gestört werden und es kann zur Bildung von Tumoren kommen. Als Zweites zu nennen sind Entzündungen, die bei der Injektion entstehen können. Ein weiterer Grund können genotoxische Stoffe in der Implantat-Hülle sein. Des Weiteren wird die elektromagnetische Strahlung als Ursprung für die Tumorbildung genannt. [7]

Es ist jedoch anzunehmen, dass die Auswirkungen der RFID Strahlung ähnliche Nebenwirkungen besitzen kann, wie es bei der Handystrahlung bekannt ist.

5.3 Retina Implantat

Da das subretinale Implantat keinerlei Schnittstelle nach außen besitzt, außer die Stromversorgung, können nur hier Angriffe erfolgen. Denkbar wäre ein Denial of Service-Angriff auf diese Stromversorgungs-schnittstelle. Das epiretinale Implantat im Gegenzug besitzt eine Wireless-Übertragung der Videodaten zum Implantat, welches als Angriffsziel verwendet werden könnte. Da das Implantat sich noch in der Forschung befindet, wurden noch keine sicherheitsrelevanten Angriffsvektoren veröffentlicht. Die nachfolgenden Angriffsszenarien bzw. Angriffs-möglichkeiten sind daher nur Vermutungen und besitzen keinen Nachweis. In der Wireless-Übertragung der Videosignale zum Implantat könnte eine Angriffsschnittstelle bestehen. Gelingt es dem Angreifer das Wireless-Signal abzugreifen, könnte dieser das sehen, was der Implantatträger sieht. Die Voraussetzung dazu müsste die passende Reichweite des Signals sein und die passende Hardware, die für das Entschlüsseln der Verschlüsselung notwendig ist. Dies birgt gerade ein Risiko, da der Angreifer auch sensible Daten wie Passwörter und PIN‘s abgreifen könnte und diese Daten für weitere Angriffe verwenden kann. Die Folgeangriffe könnten sich dadurch auf verschiedene Bereiche wie das Banking beziehen oder auf Bereiche der Spionage.

6 Fazit

Nachdem nun die verschiedenen Technologien vorgestellt und gleichzeitig die denkbaren Angriffsmöglichkeiten dargestellt wurden. ist ersichtlich, dass auch Implantate dem Risiko eines Angriffs unterliegen.

Es bleibt noch zu sagen, dass die Implantate in der Zukunft mit zunehmender Zuverlässigkeit häufiger Anwendung finden werden. Dies liegt daran, dass gerade im medizinischen Bereich die Implantate neue Möglichkeiten bieten, Menschen mit Erkrankungen zu helfen. Sei es hierbei, dass Blinde wieder etwas sehen können oder Taube wieder etwas hören. Doch gerade bei den medizinischen Implantaten, ist ein erhöhter Sicherheitsstandard von Nöten, denn gelingt es die Implantate anzugreifen, entstehen nicht nur datentechnische Schäden, die die persönlichen Informationen des Trägers betreffen, sondern auch gesundheitliche. Wie Kapitel 5.1 aufzeigt, besteht zu dem ein Risiko, dass Anschläge über die Implantate verübt werden können.

Es ist zusätzlich zu erwarten, dass es auch in der kommerziellen Ebene zu Weiterentwicklungen kommen wird. Hier könnten Systeme entwickelt werden die die gesundheitliche Überwachung übernehmen, auch wenn noch keine konkrete Erkrankung vorliegt – sie würden beispielsweise eine Weiterentwicklung der Fitnessarmbänder darstellen.

7 Literaturverzeichnis

[1] R. Münstermann, Zahnärztliche Behandlung und Begutachtung: Fehlervermeidung und Qulaitätssicherheit,2009: Georg

Thieme Verlag, ISBN978-3-13-127092-4

[2] H. Feser, Elektromagnetische Verträglichkeit,2004, VDE Verlag GmbH,ISBN: 3-8007-2810-9.

[3] F. Goss, M.Middeke, T.Mengden, N.Smetak, Praktische Telemedizin in der Kardiologie und Hypertensiologie, 2009,George Thieme Verlag KG, ISBN: 978-3-13-149931.

[4] A. Graafstra, Hands On , ISSN 0018-9235, Page 18-23, IEEE.

[5] https://www.heise.de/newsticker/meldung/Chip-Implantat-zur-Identifikation-Firma-will-Mitarbeitern-Chips-einsetzen-3780940.html , Letzter Zugriff 05.03.18

[6] http://www.spiegel.de/karriere/schweden-cyborg-firma-implantiert-mitarbeitern-mikrochips-a-1141826.html ,Letzter Zugriff 05.03.18.

[7] D. Bertschin, D.Hilber, M.Heiniger, Fallstudie Mikrossteme- Implantierte RFID-Chips und Privatsphäre,2011, Fachhochschule Norwestschweiz

[8] K. Stingl et al., Was können blinde Patienten mit dem subtextualen Alpha-IMS-Implantat im Alltag sehen, 2012, Springer Verlag, DOI 10.1007/s00347-011-2479-6

[9] K. Stingl et al, Subretinale Visuelle Implantate, 2014, Georg Thieme Verlag KG Stuttgart, DOI: 10.1055/s-0029-1245830

[10] S. Kolsberg, Drahtlose Signal- und Energieübertragung mit Hilfe von Hochfrequenztechnik in CMOS Sensorsystemen, 2002, Fraunhofer IRB Verlag, ISBN 978-3-8167-6129-7.

[11] G. Roessler et al, Implantation and Explantation of a Wireless Epiretinal Retina Implant Device: Observationduring the EPIRET3 Prospective Clinical Trial,2009, Invest Ophthalmol Vis Sci, doi:10.1167/iovs.08-2752

[12] S. Busse, K. Beer, Modernes Leben-Leben in der Moderne, 2017, Springer Fachmedien Wiesbaden, ISBN: 978-3-658-13751-9

[13] M. Goodman, Global Hack: Hacker, die Banken ausspähen, Cyber-Terroristen, die Atomkraftwerke kapern, Geheimdienste, die unsere Handys knacken, 2015, Carl Hanser Verlag, ISBN: 978-3-446-44463

[14] Beitrag von: Judith Horchert, Spiegel Online, http://www.t-online.de/digital/sicherheit/id_76509912/herzschrittmacher-hacken-die-sicherheitsluecke-im-brustkorb.html, letzter Zugriff (29.03.2018)

[15] K. Finkenzeller, RFID-Handbuch: Grundlagen und praktische Anwendungen von Transpondern, kontaktlosen Chipkarten und NFC:2015, Carl Hanser Verlag, ISBN: 978-3-446-43943-6

[16] T. Schrödel, Ich glaube, es hackt!: Einblick auf die irrwitzige Realität der IT-Sicherheit:2014, Springer Fachmedien, ISBN: 978-3-658-04245-5

[17] Bildquelle: Chaostreff Bern https://www.chaostreffbern.ch/rfid_report.html: Letzter Zugriff 05.03.18

[18] EC Council, Ethical Hacking and Countermeasures: Linux Macintosh and Mobile Systems,EC Council, 2010, ISBN: 978-1-4354-8364-4

[19] M. Rieback, P. Simpson, B.Crispo, A.Tanenbaum, RFID malware: Design principles and examples, 2006, doi:10.1016/j.pmcj.2006.07.00