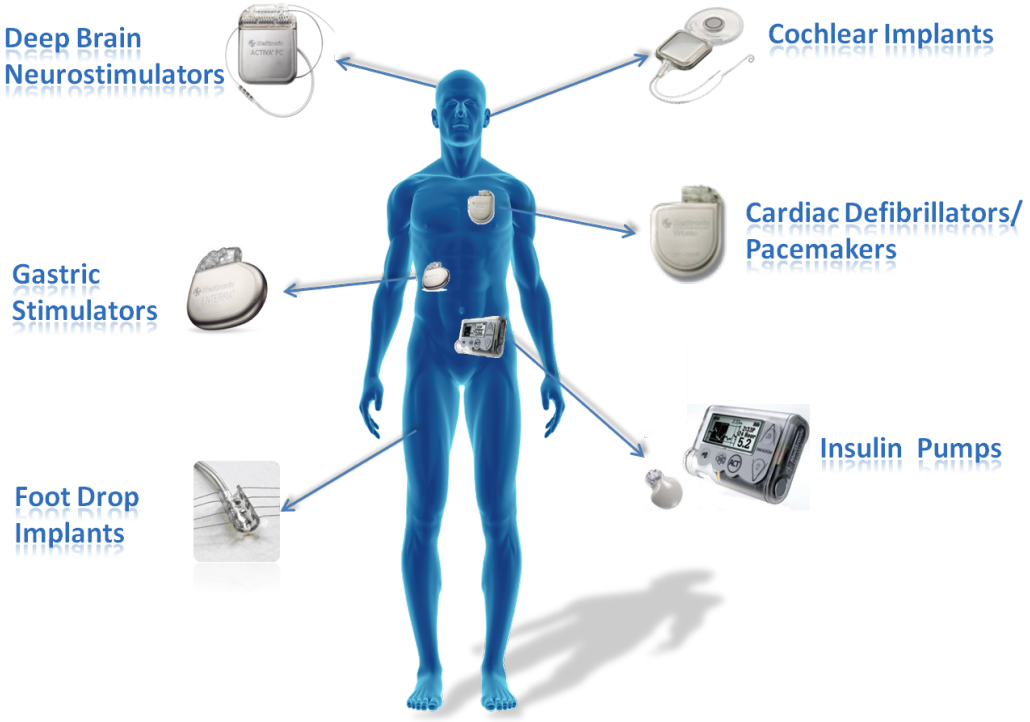
Sikkerhed i medicinske apparater

Masterprojekt - softwarekonstruktion



Af Ulrik Møller Jakobsen
Studienummer: 20160599

Master-IT
Aalborg Universitet
6/12-2017

Resumé

Since 1998 I have been an ICD-pacemaker user. This has left me with a lot of questions about the general security in the system I now have implemented in my body. In this report I describe what an ICD-pacemaker is and what positive and negative impact the wireless functions in medical devices is having on patients, designers and doctors. In this Master thesis I have used the methods from three pillars of software security and the FIT model acquired from the Masters education to analyse the security in medical devices. I have done risk analyses of the ICD device I have implanted and found that a lot of attacks was proven possible, but still no actual attacks has been reported. The patient's safety is an important factor when designing medical devices. This report describes why it’s important and take a look at examples of new future security mechanisms that allow the developer to keep the security high without lowering the patient safety. None of these mechanisms are on the market yet but maybe in the future we will see some great new standards to use when developing medical devices. Many of these devices are designed to improve the patient's lives or even keep them alive. If that's no longer possible because of too many advanced security mechanisms the whole purpose of the device is no longer existing.
I have looked into FDA’s recommendation guidelines on how to design manage cybersecurity in medical devices. The FDA guidelines is a list of different guidelines to follow to help develop secure software for medical devices. Compared to the three pillars of software security the FDA guideline is designed for medical wireless devices in general and that's why it’s the one I would recommend to use for design of ICD-pacemakers. Both guidelines are very good, easy to use and let the user decide what parts of it to use. Working with this Master thesis has given me a better understanding of what problems the developers are facing when designing systems for medical devices. A very interesting problem that I didn't think of before is the importance of patient safety vs security and why it's not possible to just add all the same security mechanisms that you would add when developing a secure system. It has been good to see that a lot is done to invent new safety mechanisms and creating guidelines for developing secure systems like the FDA and the three pillar guidelines.

1 Indholdsfortegnelse

1 Indholdsfortegnelse **2**

2 Indledning **4**

3 Baggrund **5**

4 ICD-pacemaker **6**

4.1 Beskrivelse 6

4.2 Hjemmemonitorering 8

4.2.1 Før og efter 9

4.3 Angrebseksempler 10

5 Three pillars of software security **11**

5.1 Risk Management 11

5.2 Touchpoints 13

5.3 Knowledge 14

6 FIT-modellen **15**

6.1 Fortrolighed 15

6.2 Integritet 15

6.3 Tilgængelighed 15

7 Patientsikkerhed **16**

8 Risikovurdering af ICD-pacemaker **17**

8.1 Angrebsvektorer 17

8.1.1 Ændre indstillinger via trådløs interface 17

8.1.2 Reverse engineering af transmitter 19

8.1.3 Deaktivering med magnet 19

8.1.4 Dræning af batteri 21

8.1.5 Opfange hjemmemonitoreringsdata 22

8.1.6 Stjæle aflæsningsudstyr 23

8.1.7 Radiobølgeangreb 25

8.2 Konklusion 26

9 Sikkerhed eller patientsikkerhed **27**

10 Patientsikkerhedsmekanismer **28**

10.1 No Security 28

10.2 Auditing 28

10.3 Krypteringsmekanismer 29

10.3.1 Public-nøgle 29

10.3.2 Symmetrisk nøgle 29

10.4 Nøgleopbevaring 30
10.4.1 Halskæde 30
10.4.2 Tatovering 30
10.5 Cloaker 30
10.6 Startknap 31
10.7 Biometrics 31
10.8 Anomaly detection 31
10.9 BTG policies 32
10.10 Oversigt 34
10.11 Konklusion 34
10.11.1 Min erfaring 35
11 Udvikling af medicinske apparater 36
11.1 FDA premarket guideline 36
11.1.1 Identificere 37
11.1.2 Beskytte 37
11.1.3 Detektere 37
11.1.4 Reagere 37
11.1.5 Genskabe 37
11.2 FDA Post Market principper 38
11.2.1 ISAO 38
11.2.2 Risk management 38
11.2.2.1 Common Vulnerability Scoring System 39
11.2.2.2 Patientsikkerhed 40
11.2.3 Rapportering 40
11.3 FDA vs three Pillars 41
12 Konklusion 42
13 Referencer 44

2 Indledning

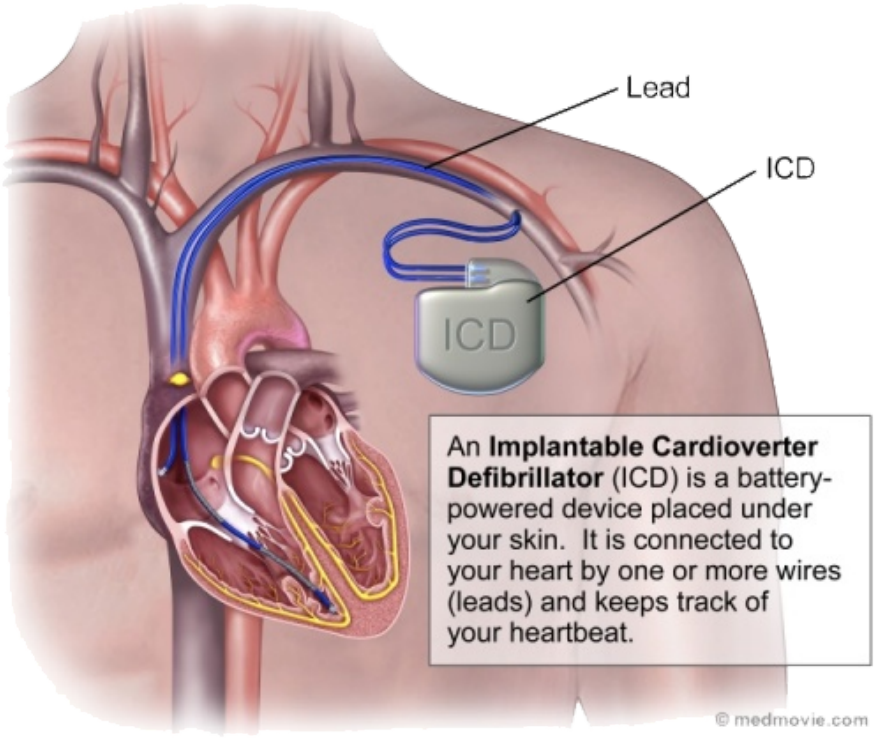
Det er blevet populært at udvikle medicinske apparater indopereret i patienter, som kan forbinde direkte til sygehuset. Grunden til dette er, at det kan give patienterne en bedre behandling idet, at de kan blive monitoreret og behandlet i deres eget hjem. Dermed slipper de for unødvendig tid brugt på kontroller og behandlinger, hvor de tidligere skulle møde op på hospitalet. Forbindelsen mellem sygehus og patienten kan bruges enten til at overvåge patienters tilstand eller på anden måde justere deres behandling. Disse apparater kan blandt andet have forbindelse til hospitalet via internettet eller et GSM-modem. Jeg er en blandt flere tusinde danskere, der har en såkaldt ICD-pacemaker indopereret. Samtidig med at sygehuset bliver bedre til at behandle og overvåge folks tilstande, kommer der desværre også flere sikkerhedshuller som en eventuel ondsindet angriber kan udnytte. Mange har meget stor værdi af disse nye behandlingstilbud, som kan spare patienter, sygeplejersker og læger for brug af unødvendig tid og penge til kontrol og transport. Dette kan medføre et fald i sikkerheden men til gengæld får patienterne en bedre og hurtigere behandling. I denne rapport bruger jeg nogle af de metoder og teknikker jeg har tillært mig i løbet af mit master forløb til at analysere og vurdere sikkerheden i min egen ICD-pacemaker. Jeg kommer ind på, hvorfor patientsikkerheden er meget vigtigt, og hvorfor sikkerheden ikke altid kommer i første række, når det gælder medicinske apparater. Jeg vil også sammenligne three pillars of software security fra undervisningen [2] [4] med FDA's egen anbefaling [11] [18] til udvikling af medicinske apparater.

3 Baggrund

For snart 20 år siden fik jeg som 18-årig indopereret en ICD-pacemaker, som skulle overvåge og behandle min hjerterytme, hvis den blev for høj. Tidligere havde jeg haft problemer med anfald med uregelmæssig hjerterytme, som kunne blive så hurtig, at lægerne mente, der var risiko for hjertestop. Gennem årene har jeg lært at leve med den og har haft stor glæde af hjemmemonitorering. Jeg indtil videre fået min ICD-pacemaker skiftet to gange, da den var løbet tør for strøm. Jeg har aldrig tidligere tvivlet på sikkerheden i den enhed, jeg har indopereret, og jeg har altid tænkt, at selvfølgelig kan den ikke hackes. Jeg bildte mig selv ind, at min ICD-pacemaker var produceret med samme høje kvalitet og sikkerhed, som når der udvikles hardware og software til fly eller rumfartøjer. De gange jeg har spurgt ind til sikkerheden har lægerne forklaret mig, at der ikke kunne ske fejl, og jeg bare skulle tage det roligt og lade dem bestemme. Det var først da jeg fik min tredje pacemaker, at jeg kom til at tvivle lidt på, om lægerne nu også vidste hvad de talte om. Denne nye model havde en smart boks, som jeg kunne få med hjem, og så ville sygehuset hver nat modtage data direkte fra min ICD-pacemaker. Via et GSM-modem bliver dagens testdata og informationer sendt direkte til hospitalet. Nu gik jeg pludselig rundt med et trådløst interfaces i brystet som var tilkoblet mit mest vigtige organ. Alt dette var sket uden at nogen havde spurgt eller informeret mig om det forinden. Jeg har fået mange spørgsmål fra venner og kolleger om sikkerheden i sådan en pacemaker og efter, at jeg er begyndt på min masteruddannelse, er jeg selv blevet mere nysgerrig. Er ICD-pacemakeren nu også så sikker og fejlfri som jeg gik og troede?

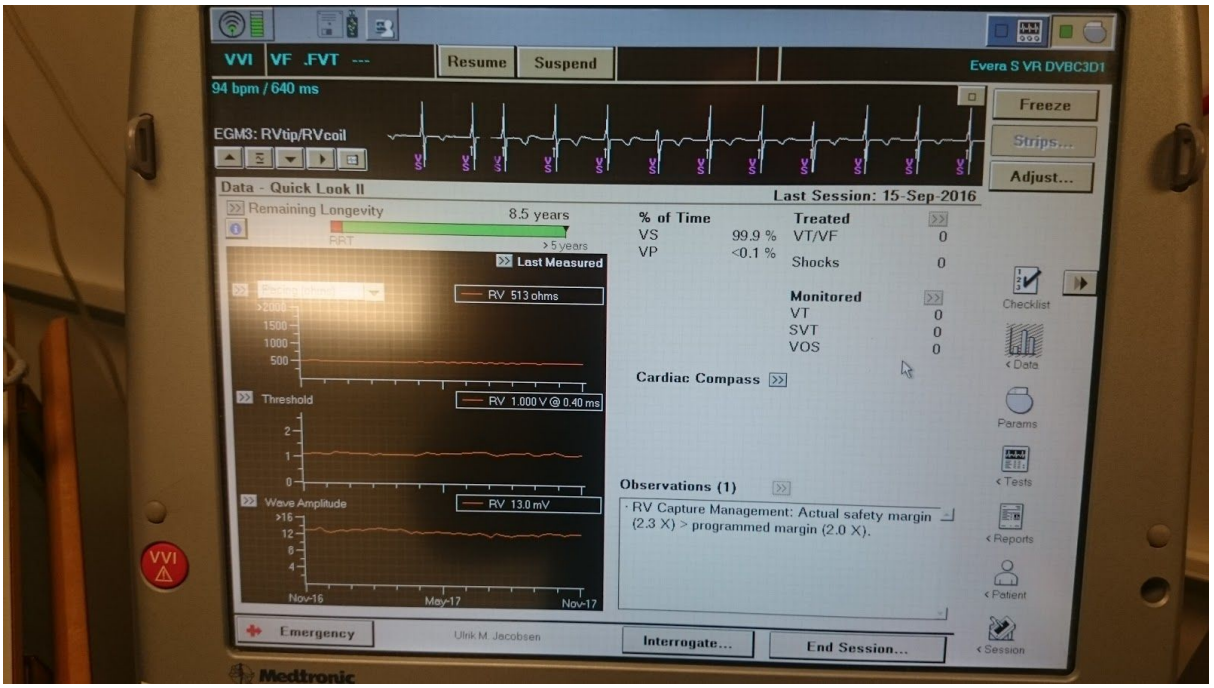
4 ICD-pacemaker

4.1 Beskrivelse



Figur 1: ICD-pacemaker (http://nyheartfailure.com/defibrillator)

En ICD-pacemaker er et apparat som minder meget om en almindelig pacemaker. Den er på størrelse med en Zippo-lighter, og er indopereret under huden i brystet. Forskellen på en ICD og en almindelig pacemaker er, at en ICD ikke hjælper hjertet med at slå, men kun overvåger hjerterytmen og vurderer om den er normal. Hvis rytmen afviger til en farlig rytme kan ICD'en behandle patienten for igen at opnå en normal rytme. Behandlingen kan ske ved at ICD'en først prøver at pace hjertet og ved at ændre rytmen i pacingen føre rytmen tilbage til den normale rytme. Hvis dette ikke er tilstrækkeligt, kan ICD'en i sidste lave en reboot af hjertet. Dette gøres ved at nulstille hjertet med et stød præcis som det en defibrillator giver når den skal genstarte et hjerte.



Figur 2: Kontrol på Skejby sygehus

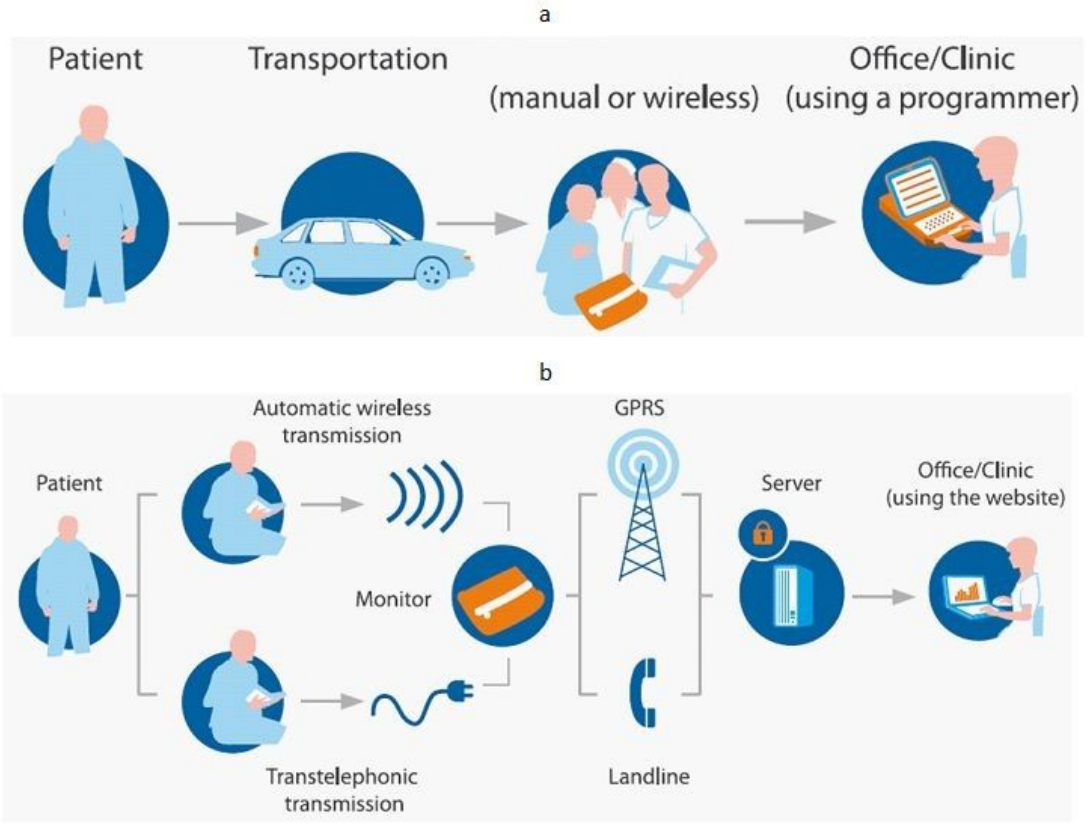
Her ses et billede af aflæsningsapparatet, som min ICD bliver aflæst med. Billedet er fra min sidste kontrol på Skejby Sygehus, og viser blandt andet, at der er ca 8,5 års batterilevetid tilbage. Der er også forskellige menuer, hvor diverse indstillinger for hvordan, enheden skal overvåge og behandle mit hjerte kan ændres.

4.2 Hjemmemonitorering

Figur 3: Aflæsningsenhed til hjemmemonitorering

Hjemmemonitorering er et tilbud til brugere af de nyere ICD-pacemakere, hvor patienters tilstand kan blive overvåget i deres eget hjem. Dette foregår ved, at man har en lille boks placeret i sit soveværelse, som hver nat tester den indopererede ICD. Hvis der er noget usædvanligt, rapporteres dette via GSM-modem til hospitalet. Dette kan betyde, at patienten bliver ringet op om morgenen og informeret om, at der har været en episode i løbet af natten, og at patienten skal møde op på hospitalet til nærmere undersøgelse. Tidligere versioner har været meget mere simple end den nye version, som ses på billedet. Den forrige version jeg havde bestod af en boks med et kabel, som gik over i et eksternt GSM-modem med et frit tilgængeligt simkort i siden.

4.2.1 Før og efter



Figur 4: Patient hjemmemonitorering
(https://www.intechopen.com/books/cardiac-defibrillation/icd-in-the-era-of-telecardiology)

Her er et billede, der sammenligner en patients faste kontrolforløb med hjemmemonitorering og uden hjemmemonitorering. Det kan hurtig ses, at der spares meget tid og mange ressourcer for både patient og sygehusvæsenet. Dette er også noget, jeg personligt er rigtig glad for, at jeg er begyndt at bruge. På denne måde bliver jeg ikke så ofte som tidligere mindet om, at jeg faktisk har en ICD. Tidligere skulle jeg til kontrol 2 til 3 gange om året alt efter hvordan det gik. Nu kan jeg nøjes med hvert andet år.
Del "a" på ovenstående billede viser, hvordan man tidligere fik sin ICD aflæst. Der skulle bruges tid på at arrangere et tidspunkt for kontrol på sygehuset. Patienten skal holde fri fra arbejde samt bruge transport til og fra sygehuset på den pågældende dag. Først herefter kan ICD-enheden aflæses og eventuelt få nye indstillinger.
Del "b" viser, hvordan enheden med hjemmemonitorering kan blive aflæst og sendt direkte til hospitalet. ICD'en bliver om natten testet samt aflæst via det trådløse interface. Hvis man selv ønsker at tvinge en afsending afsted indeholdende nuværende tilstand, er der på

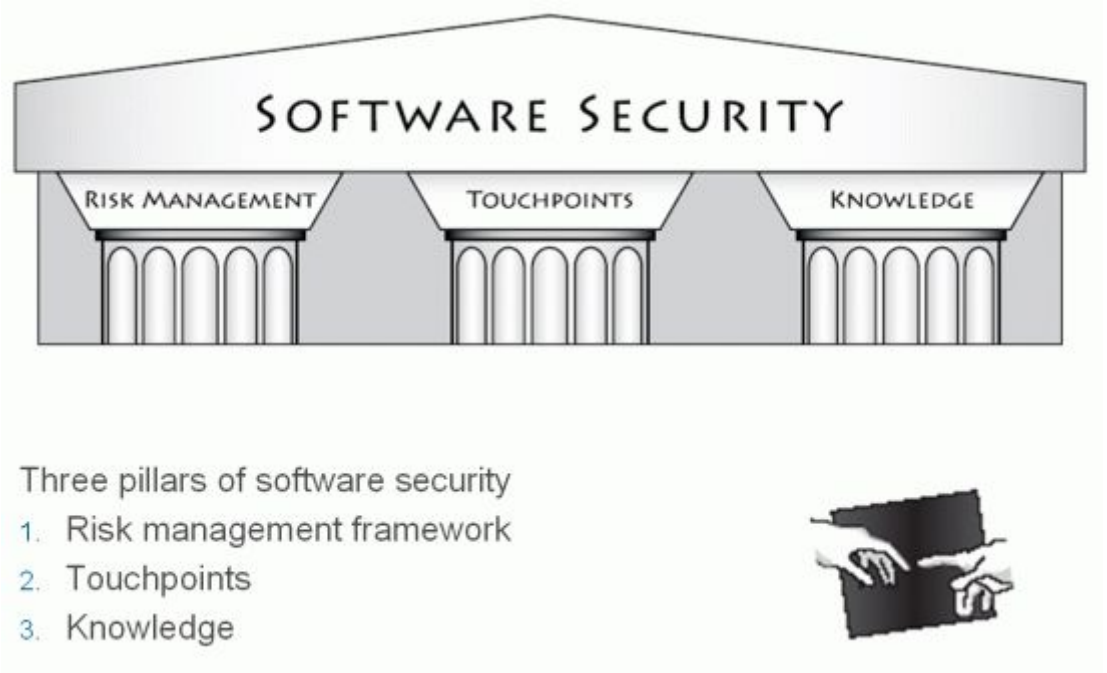
apparatet en aflæsningsenhed som kan placeres over ICD-pacemakeren og via transtelephonic [3] sende direkte til hospitalet. Her er det vigtigt at bemærke, hvor meget tid og penge en sådan feature sparer for både hospitalet og patienten. Det er også en meget hurtigere og bedre behandling, patienten får, da der hurtigt kan stilles ind til den mest optimale behandling for den pågældende patient. Alt dette skal tages med i de senere overvejelserne for, hvor vigtigt det er at have høj sikkerhed i systemet, kontra hvor meget værdi en feature kan give. Det kunne jo være, at man kunne leve med en lidt lavere sikkerhedsniveau og gøre hverdagen nemmere og billigere for alle parter.

4.3 Angrebseksempler

Der findes forskellige eksempler på, at det er blevet bevist muligt at hacke pacemakere. Allerede i 2008 udgav Daniel Halperin en artikel [8] ”*Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses”,*
som beskriver, hvordan han - og en række researchere - kunne hacke en ICD-pacemaker ved brug af radiobølger. Dermed var det muligt at ændre indstillinger på denne, som kunne være livstruende for patienten. Dette angreb kræver dog, at man er helt tæt på patienten, for at det kan udføres. Et andet eksempel er Hackeren Barnaby Jack, som i 2013 havde fundet en måde, hvorpå han trådløst kunne hacke pacemakere indenfor en radius af 15 meter [9]. Desværre nåede han ikke at udgive sit arbejde, da han - 3 dage inden fremlæggelsen var planlagt - desværre døde. Et nyere eksempel er Marie Moe [5] [10] [14], som efter hun selv har fået en pacemaker er begyndt at forske i, hvor sikker hendes pacemaker er. Hun har sammen med sit team haft succes med at hacke diverse pacemakere. Hun holder spændende forelæsninger om deres arbejde og om hendes egen rejse som pacemakerbruger. Der er også lavet en analyse af sikkerhedsbrister i den aflæsningsenhed, som bruges af hospitaler til at forbinde til patienters Pacemakere. Her viste der sig et tydeligt billede af, at der var mange brister som ville være lette at udnytte [17] [19]. Et andet eksempel er fra 2017, hvor FDA tilbagekalder 500.000 pacemakere. Der blev fundet en sikkerhedsbrist som gjorde at en angriber med “standardudstyr” kunne ændre indstillinger på pacemakere [24]. Heldigvis blev fejlen fundet, og det var muligt at rette den med en firmwareopdatering.

5 Three pillars of software security

Som en del af masterundervisningen for fagpakken “sikker software udvikling” lærte jeg om “the three pillars of software security” [2] [4]. Det handler om tre grundlæggende punkter som kan benyttes til at forbedre sikkerheden, når man udvikler software. Her vil jeg kort beskrive, hvad de tre punkter går ud på, og senere vil jeg benytte nogle af metoderne til at analysere sikkerheden i min egen ICD-pacemaker.

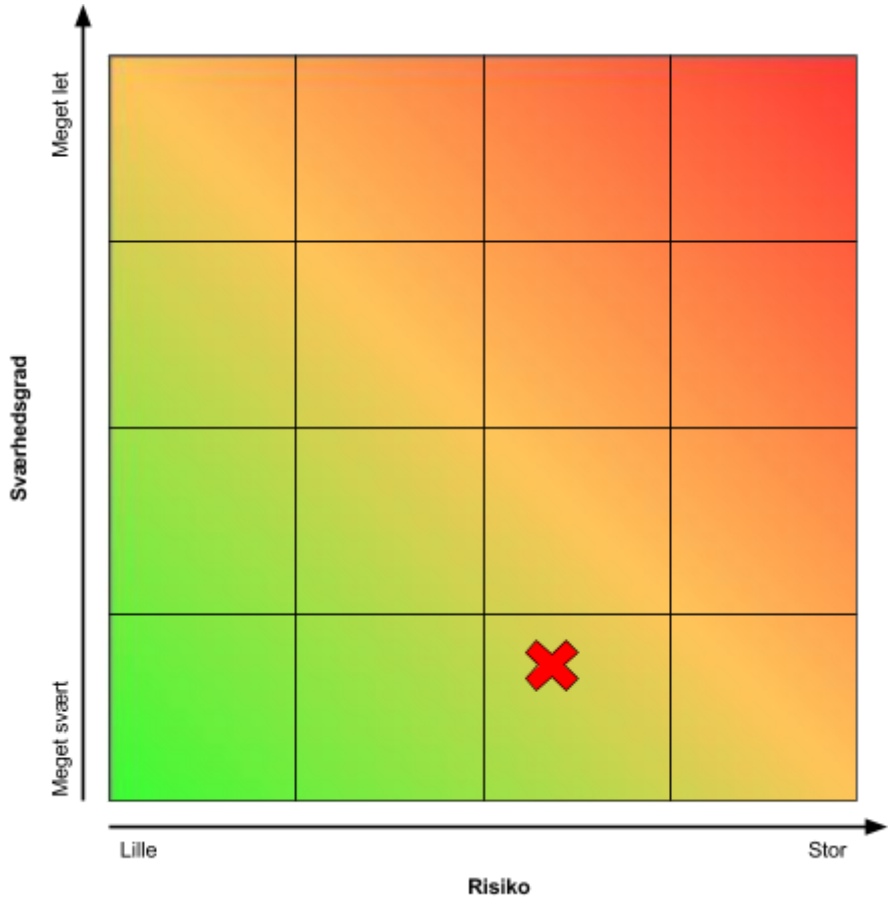


Figur 5: Three pillars of software security (http://www.swsec.com/resources/pillars/)

5.1 Risk Management

Den første af de tre søjler hedder risk management. Det går ud på, at man skal have indført en kontinuerlig process, hvori man får analyseret og håndteret alle de tænkte sikkerhedstrusler, der kan findes mod ens system. Trusler kan findes på flere forskellige måder lige fra brainstorm til indhentning af viden fra diverse sikkerhedsforums. Man kan selv tilpasse alt efter hvad man synes passer til ens ambitionsniveau og kompetencer. Der findes også tjeklister, man kan bruge som inspiration til at komme igang. Det er også altid en mulighed at få et eksternt firma til at lave analysen for en. Man skal bare huske, at det ikke er noget der kun skal laves en gang. Det skal helst være en proces som køres igen og igen,

hvor gamle kendte trusler genvurderes samt nye trusler tilføjes til listen. Hvert af de fundne trusler skal individuelt vurderes, og får en score på to punkter. Det første punkt er sværhedsgraden af udførelse af angrebet altså hvor svært er det at udføre. Hvis det er noget som kun de mest hardcore hackere med specialudstyr og mange millioner på kontoen kan udføre, så får det en lav score. Hvis det er et angreb som alle og enhver kan udføre ved at downloade et program og hacke systemet med et enkelt tryk, så får det en høj score. Det andet punkt, der skal vurderes på er, hvor slemt det ville være, hvis angrebet faktisk skete. Betyder udførelse af angrebet, at patientens monitoreringsdata kan ses af andre i et kort øjeblik, så er vurderingen i den lave ende. Hvis det modsat er et angreb, som patienten kan dø af, så får den en score i den høje ende.

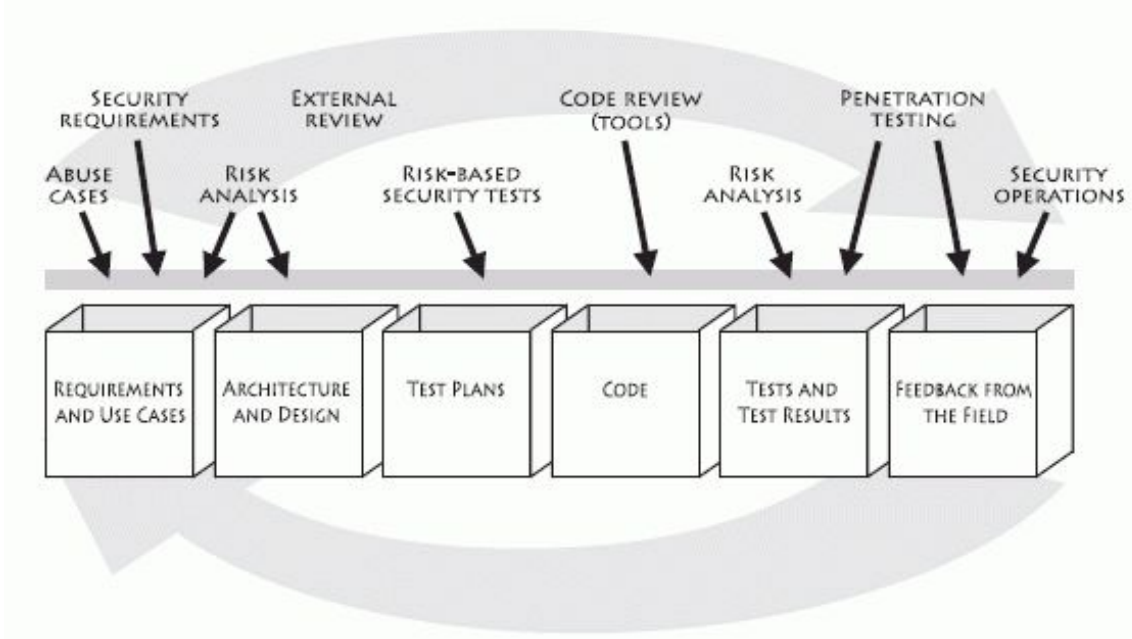


Figur 6: Graf til risikohåndtering

De to tal for hver kendt sikkerhedstrussel indsættes på en graf med sværhedsgrad af angrebet som Y-akse, og risiko hvis angrebet sker som X-akse. Denne graf giver en nem måde at se, hvilke trusler man burde tage fat i først, og hvilke det ikke giver nogen mening at

bruge ressourcer på at rette i første omgang. Dette er også et godt værktøj til at vise ledelsen, hvilke trusler man kender og få dem til at forstå, at det er nødvendigt at investere i at få håndteret de trusler, der nærmer sig det øverste røde hjørne til højre.
En god ide' vil være at implementere risk management som en del af sin daglige strategi og udviklingsplan med eventuelle ugentlige møder med alle sikkerhedsinteressenter i organisationen. Jeg vil i denne masteropgave bruge risk management af denne type til at finde og vurdere angrebstrusler mod min ICD-pacemaker. Hver fundet sikkerhedsrisiko vil jeg give en beskrivelse af samt min personlige vurdering af, hvorfor jeg placerer den hvor jeg gør på grafen.

5.2 Touchpoints



Figur 7: Touchpoints (http://www.swsec.com/resources/pillars/)

På ovenstående figur ses de syv touchpoints som er "abuse cases", "security requirements", "risk analysis", "risk based security tests", "code review", "penetration testing" og "security operations". På billedet kan man også se hvilke faser af udviklingen de enkelte punkter tilhører. For at gøre det nemmere at få indført en proces hvor alle parter i udviklingsprocessen husker at tænke på sikkerhed, kan det være en god ide' at udarbejde guidelines som kan hjælpe medarbejdere med at huske de vigtigste områder inden for de enkelte touchpoints. Dog skal man huske, at det ikke skal blive en tjekliste, som man bare

følger og slavisk udfører hvert punkt. Det skal være punkter som giver mening og bruges som inspiration. Alle punkter skal løbende revurderes og eventuelt tilpasses, når vi bliver klogere og opdager nye risici. I dette projekt vil jeg sammenligne de syv touchpoints med FDA's forslag til hvordan systemer indenfor medicinske apparater burde udvikles. Vidensdeling og søgen efter ny viden er vigtigt inden for sikkerhed og hvert af de syv touchpoints kræver, at man hele tiden får sin viden om sikkerhed opdateret. Dette bringer os videre til det tredje og sidste punkt af de tre touchpoints nemlig viden.

5.3 Knowledge

Viden er en essentiel del af sikkerhed. Man skal hele tiden holde sig opdateret, da man skal vide, hvad man skal beskytte sig imod. Det, der tidligere blev anset for sikkert, kan i dag være blevet brudt. Samtidig med, at hardware bliver hurtigere og hurtigere, vil systemer blive nemmere hacke, hvis ikke de følger med tiden. Det er svært at forudse, hvad der præcis vil ske i fremtiden, så derfor er det vigtigt at holde sin sikkerhedsviden opdateret. Viden kan være mange ting. Det kan blandt andet være undervisning af medarbejdere, specialister eller brugere af ens system. Viden kan også være at tilmelde sig en masterfagpakke. Det er hele tiden et kapløb om, at når en sikkerhedsbrist bliver opdaget, skal den risikovurderes og håndteres hurtigere, end angriberne kan nå udnytte det.

6 FIT-modellen

I undervisningen på fagpakken “sikker software udvikling” lærte vi også om en af grundstenene indenfor sikkerhed, nemlig FIT-modellen eller på engelsk CIA. Denne model beskriver de områder, som eventuelle sikkerhedsbrister eller angreb kan ramme ens system på. Forkortelsen FIT står for fortrolighed, integritet og tilgængelighed. Herunder vil jeg kort beskrive hvert punkt, og senere i risikovurderingen af min ICD-pacemaker vil jeg benytte FIT modellen til vurdering af de fundne sikkerhedstrusler.

6.1 Fortrolighed

Første punkt i FIT modellen er fortrolighed. Det skal ikke være muligt for en angriber at læse ens information eller på anden måde vide noget om, hvad man foretager sig. Et eksempel kan være hemmelige dokumenter, passwords eller andre vigtige informationer, som man ikke ønsker at dele med andre. En måde at undgå dette på kan være ved at kryptere sine hemmeligheder.

6.2 Integritet

Hvis det lykkes for en angriber at ændre i ens informationer, er integriteten brudt. Et godt eksempel på dette er et banksystem eller en bankoverførsel, hvor det er yderst vigtigt, at der ikke kan ændres på data. Ændres et enkelt tal i en bankoverførsel, kan det have meget store konsekvenser for enten størrelsen på beløbet, der overføres, eller kontoen, der overføres til. Derfor er det altid en god ide’ at validere data. En måde at gøre det på kan være at have en hashværdi af den kommando, man sender til banken og så tjekke, at den stadig er det samme, når banken modtager og udfører kommandoen.

6.3 Tilgængelighed

Det er vigtigt, at et system er tilgængeligt, når man skal bruge det. Specielt indenfor medicinske apparater, hvor det kan medføre risiko for patienters liv. Nedetiden er også en vigtig parameter i konkurrencen mellem forskellige services, og manglende tilgængelighed kan være en dyr affære. Et værn mod dette kan blandt andet være at have en god backupstrategi med hyppige backups og flere servere, som systemet automatisk kan skifte imellem ved nedbrud.

7 Patientsikkerhed

Indenfor medicinske apparater er det ikke kun FIT-modellens punkter man kan blive ramt på. Et fjerde punkt som vi til dagligt ikke har ret stor fokus på indenfor IT sikkerhed er patientsikkerheden. Patientens sikkerhed er gerne den faktor, der i første omgang er skyld i at patienten overhovedet har brug for hjælp fra diverse apparater. Hvad nytter det, at en patients data er beskyttet, hvis ikke det er muligt at få den behandling, som apparatet er designet til at give? Man kan groft sagt sige, at patienten skal holdes i live, for at alt andet sikkerhed giver nogen mening. Flere af de sikkerhedsmetoder man benytter indenfor nutidens software og webapplikationer kan ikke bruges, da strømforbrug og batterilevetid er en vigtig faktor. Alt, der kan udnyttes til at dræne batterier, er en trussel mod patientsikkerheden. Det kræver en operation at skifte et batteri i en ICD-pacemaker, og ved enhver operation er der en risiko for komplikationer. Et eksempel på teknologier, som ikke egner sig til medicinske apparater er SSL-teknologien, som bruges til at oprette krypterede forbindelser til websider. Her bliver der brugt mange kald frem og tilbage for at oprette en sikker forbindelse. Dette vil ikke kunne bruges i medicinske apparater, da der skal spares på både regnekraft og båndbredde, for at kunne spare på batteriet. Hvis en angriber finder på at spamme en sådan service skal der bruges regnekraft og batteri på uautoriserede kald, som til sidst kan gå hen og dræne systemet. Jeg vil senere se på nye sikkerhedsmekanismer, til medicinske apparater, som kan styrke både sikkerheden og patientsikkerheden.

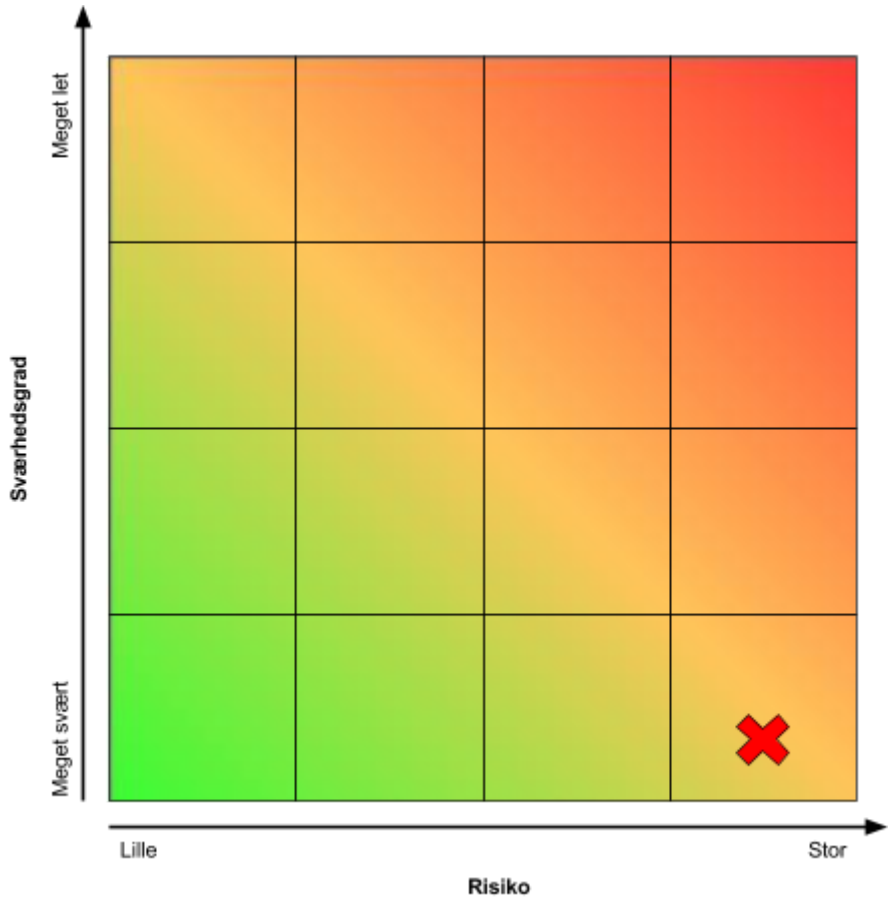
8 Risikovurdering af ICD-pacemaker

8.1 Angrebsvektorer

Her vil jeg beskrive nogle af de tænkte angreb, der kunne komme imod en ICD-pacemaker som den, jeg har indopereret. Det er ikke en komplet liste, og skal ses som en liste der løbende bliver opdateret med nye tænkelige angreb. Eksempelvis kan der findes et angreb som i dag ikke er bevist muligt. På et senere tidspunkt bliver angrebet muligt, da angriberen også bliver klogere og opfinder nye angreb. For hvert angreb, jeg finder, vil jeg ud fra FIT-modellen og patientsikkerheden vurdere, hvordan brugeren af ICD'en vil blive ramt. Dette bruges til vurdering af hvor i risikografen angrebet skal placeres.

8.1.1 Ændre indstillinger via trådløs interface

En angriber der er indenfor rækkevidde af et ICD apparatet kan bryde krypteringen, der bruges over den trådløse forbindelse og få direkte adgang til enheden. Herefter kan angriberen ændre på diverse livstruende indstillinger eller i værste fald helt slå ICD'en fra. Når angriberen som i dette eksempel får fuld adgang til enheden, kan angrebet få store konsekvenser. Dette rammer flere dele af FIT-modellen, men først og fremmest er det *integriteten*, det går ud over, da angriberen kan ændre indstillinger. Hvis han vælger at slukke helt for enheden, er det *tilgængeligheden* det går ud over, og dette vil have en indflydelse på patientsikkerheden.

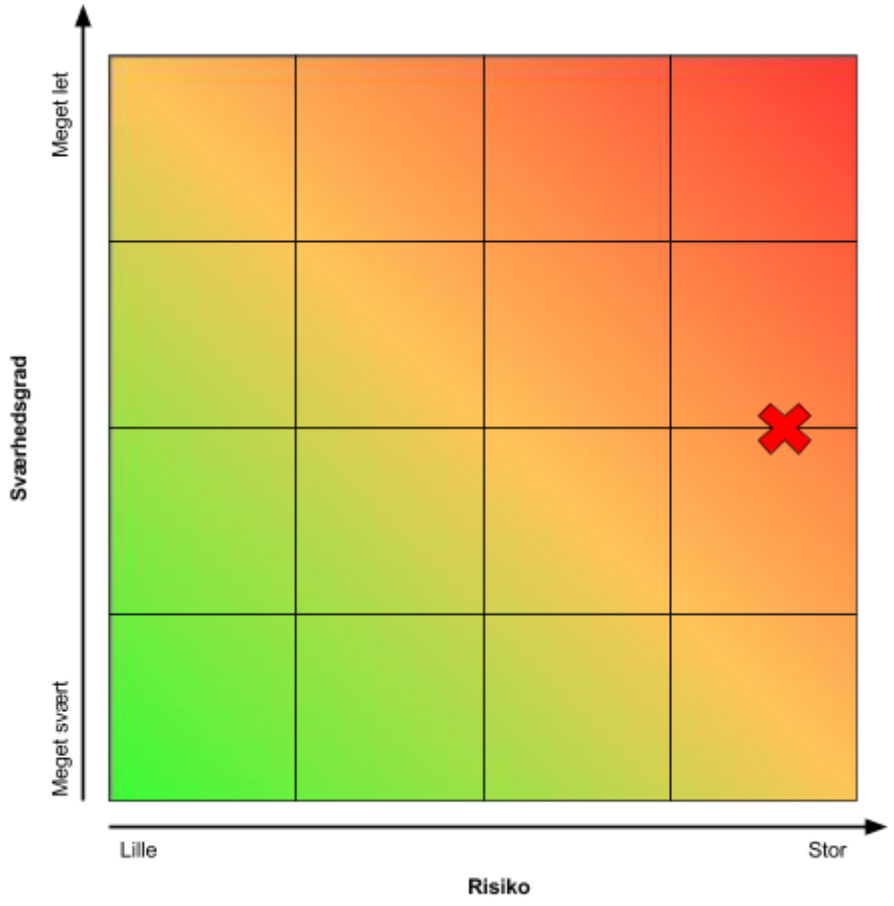


Figur 8: Graf - ændre indstillinger via trådløs forbindelse

Denne form for angreb vil have store konsekvenser for både patient og pacemaker-fabrikanten. Det kan i værste fald være livstruende for patienten og dette i sig selv gør, at risikoen bliver placeret tæt på maks. Det vil også være problematisk for fabrikanten hvis det f.eks kom frem i pressen, at det var et nemt angreb. Dette kunne medføre, at alle patienter skulle indkaldes til en operation for at få udskiftet deres ICD-pacemaker. Heldigvis er angrebet svært at udføre, og der har indtil videre ikke været kendte angreb af denne type. Dem som har haft succes med at bevise denne type angreb har været tæt på patienten og haft al den tid der var nødvendig. Min vurdering af angrebets sværhedsgrad bliver, at det er meget svært at udføre. Sværhedsgraden bliver derfor placeret helt i bunden. Dette gør at krydset bliver placeret lige uden for det røde felt.

8.1.2 Reverse engineering af transmitter

Scanne område for ICD'er og forbinde med tilpasset universal hardware



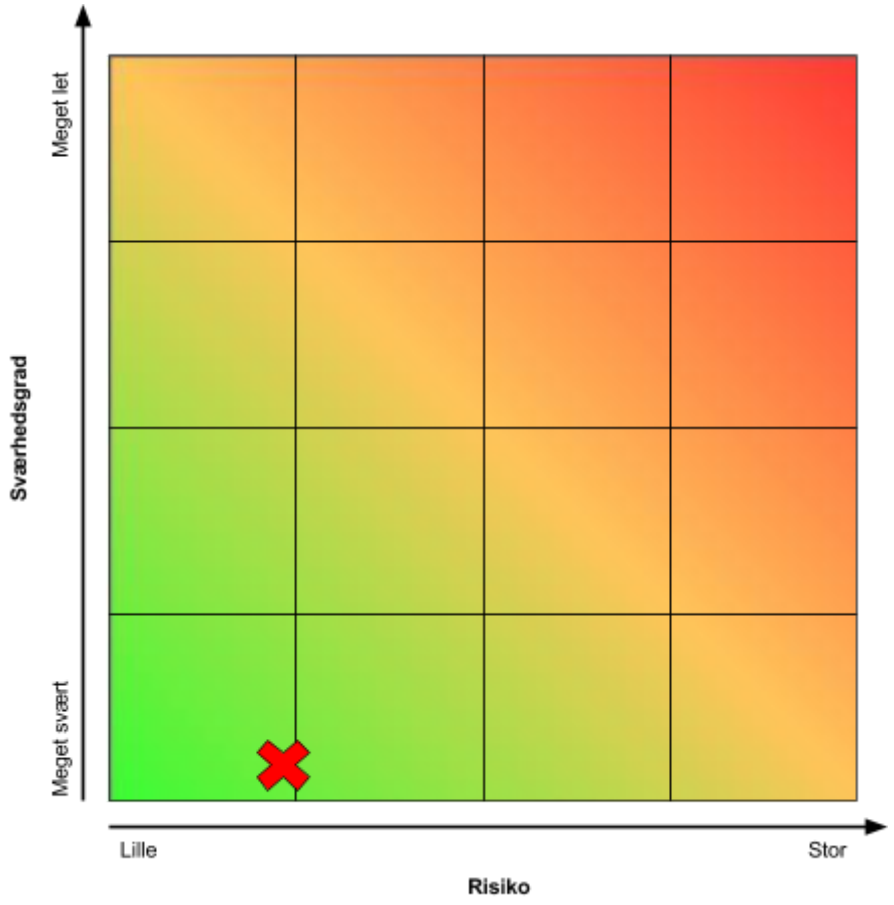
Figur 9: Graf - reverse engineerings angreb

Dette angreb vil være middelsvært at udføre men hvis det sker er risikoen meget høj. Det er i dag meget populært at angribe alle mulige IOT devices via RF, da mange producenter tror, at det er svært at lave reverse engineering på lige netop deres protokoller. En pacemaker kunne blive ramt af et sådant angreb, og konsekvenserne kan blive kolossale.

8.1.3 Deaktivering med magnet

En indbygget feature i ICD-pacemakeren er, at hvis den bliver udsat for et kraftigt magnetfelt, vil den automatisk slukke indtil den igen er udenfor magnetfeltet. Dette gøres for at undgå fejlbehandlinger som skyldes magnetens indflydelse på ICD-enheden. Dette kan let udnyttes af en angriber, som blot skal medbringe en kraftig magnet. I de senere versioner er

der dog indført en lille ændring, som gør dette angreb svært at indføre. Der er indført en hyletone, som umuligt kan blive overhørt af patienten. Dette gør at, patienten er klar over at ICD'en er slukket og selv kan flytte sig til et magnetfrit område. I dette angreb er det *tilgængeligheden,* det går ud over, da angrebet gør, at patienten ikke kan få sin behandling, så længe ICD'en er slukket.

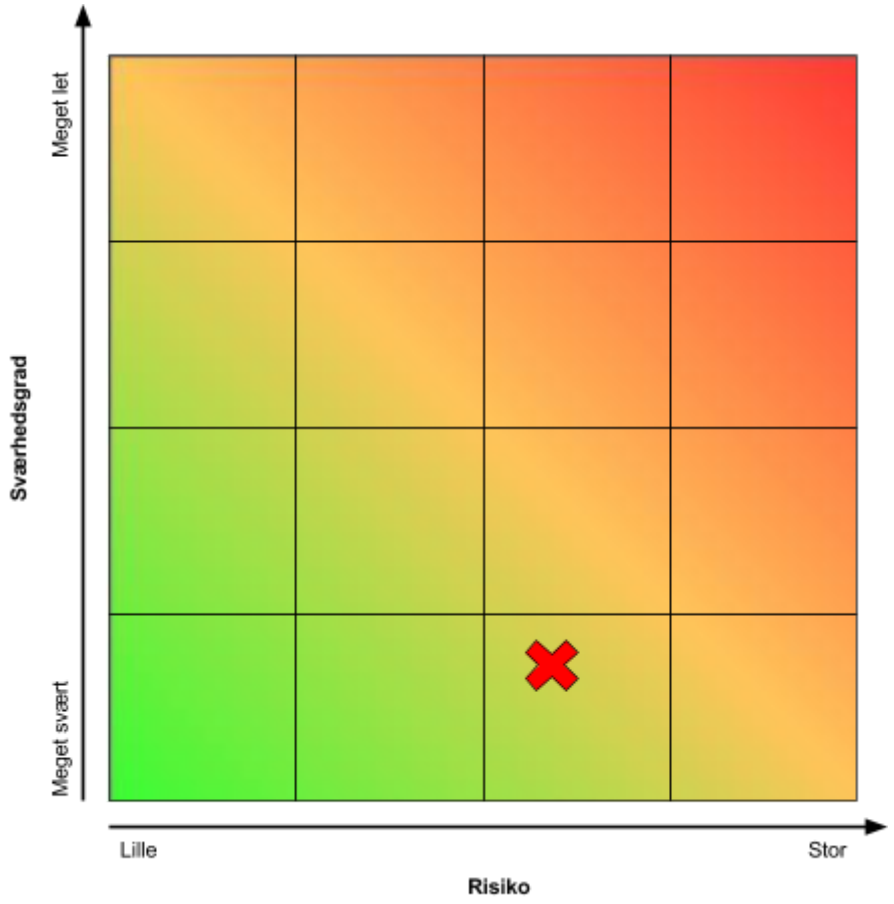


Figur 10: Graf - deaktivere ICD med magnet

Efter min vurdering er angrebet meget svært at få succes med, da angriberen skal have magneten placeret meget tæt på patienten, samt patienten skal være hørehæmmet for at overhøre alarmen. For at dette angreb bliver helt alvorligt skal det også passe sammen med, at patienten får et af de hjerterytmeanfald, som ICD'en skal behandle. Alt i alt et meget svært angreb at udføre som, højst sandsynligt ikke gør nogen skade.

8.1.4 Dræning af batteri

En anden type angreb kan opstå hvis en angriber finder en måde at lave gentagne forespørgsler over den trådløse forbindelse. Hvis disse forespørgsler får ICD-enheden til at lave nogle tunge beregninger kan dette over tid dræne batteriet. Batteriet er meget vigtigt i en ICD, og skal spares så meget på som muligt. Er der ikke mere batteri tilbage, er patientsikkerheden i fare da enheden ikke længere kan udføre sine livsvigtige behandlinger. I henhold til FIT modellen er det her *tilgængeligheden*, der bliver berørt. Der kan ikke skiftes batteri i en ICD, så eneste udvej er at via en operation at udskifte hele enheden. Som standard under normale forhold holder batteriet i en ICD 8 - 12 år.

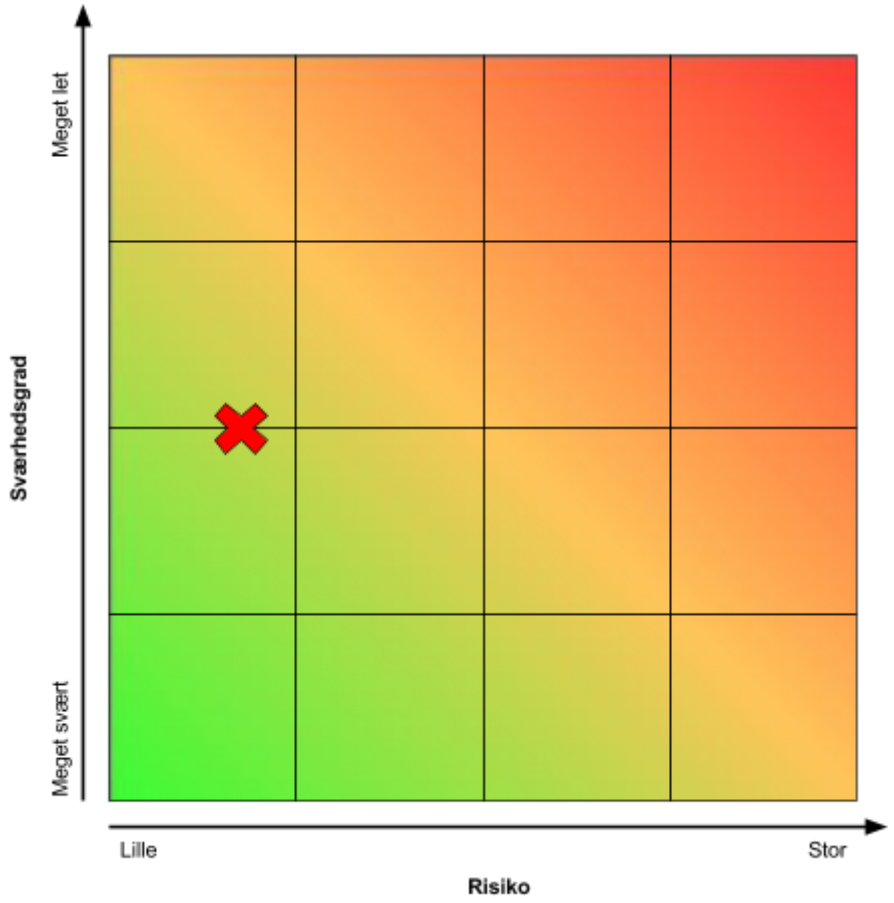


Figur 11: Graf - dræne batteri

Placeringen af krydset for dette angreb bliver lidt over middel risiko. Det store problem med dette angreb er, at der skal en operation til for at skifte batteriet, og ved en operation kan der opstå komplikationer. Denne type angreb vil højst sandsynligt blive opfanget af hjemmemonitoreringen, da man kan se et pludseligt forøget forbrug fra dag til dag, og herefter vil man blive indkaldt til en nærmere undersøgelse på hospitalet.

8.1.5 Opfange hjemmemonitoreringsdata

Via hjemmemonitorering sendes der jævnligt information om patientens tilstand til hospitalet. Denne data sendes via et GSM-modem til et hospitalet eller en server, som hospitalet kan slå patienterne op på. En angriber kan opfange denne information ved at lytte på modemet og enten se, at en person er hjemme, hvis der sendes noget, eller bryde kommunikationen og opsamle de pakker, der sendes. Dette vil give angriberen enten patientens personlige informationer om sygdommen eller om hvilke dage, patienten har været hjemme. Disse informationer kan være værdifulde i de rette personers hænder. Forsikringsselskaber vil gerne kende til deres kunders helbredsstatus, og det er set før at de tager utraditionelle metoder i brug for at opnå dette. En angriber vil gerne vide, hvilke dage man er hjemme på, hvis der netop er en bestemt dag på ugen man aldrig er hjemme, vil det være oplagt at lave indbrud på denne dag.



Figur 12: Graf - opfange hjemmemonitorerings data

Dette angreb vil jeg vurdere til at have middel sværhedsgrad at udføre. Der findes idag diverse værktøjer som alle kan downloade og bruge til at aflytte GSM-trafik [23]. Jeg har f.eks stadig boksen fra min gamle ICD-pacemaker liggende som jeg kunne lave lidt forsøg

på inden jeg begyndte at overvåge naboen. Det er også en mulighed at købe brugte apparater på eks. ebay.com [19]. Dette gør, at krydset for dette angreb bliver placeret midt på grafen for sværhedsgrad, og næsten helt i bund for risiko. Dette vil sige, at det nok ikke bliver det første punkt, der skal forbedres. Der findes eksempler på, at dette "angreb" bliver udført på lovlig vis, nemlig i retssager, hvor en mistænkts pacemakers data er blevet brugt som bevis i retten til at fælde dom [15].

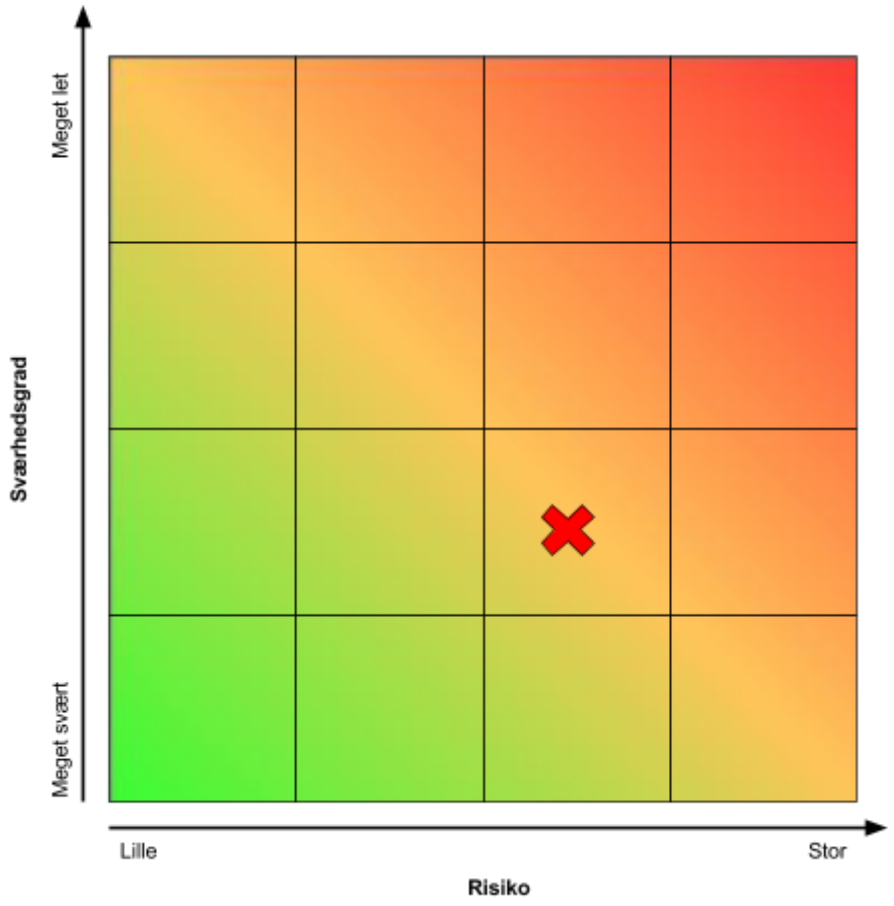
8.1.6 Stjæle aflæsningsudstyr

Hospitaler over hele verden skal kunne aflæse alle versioner af pacemakere og ICD'er. Dette skal de kunne for at patienter, som er på besøg i andre lande skal kunne få deres livsvigtig behandling eller indstillinger fra hospitalet, hvis der får brug for det.

Figur 13: Billede fra ICD-kontrol

Her er et billede fra sidst jeg var til den årlige kontrol med min egen ICD. Rummet, jeg blev behandlet i, var fyldt med forskellige typer af universal aflæsnings enheder.
Et angreb kunne være, at en angriber fysisk stjæler et sådant apparat eller låner det og laver en kopi. Rummet, hvor billedet, er taget er i hospitalets åbningstid ubemandet og ulåst, så det ville ikke kræve meget at liste ind og stikke et af apparaterne i sin taske.

Når angriberen så har apparatet, kan det bruges til at aflæse patienter inden for rækkevidde. Et eksempel kunne være i et tog eller bus, hvor angriberen sidder bagved og aflæser eller indstiller ICD'en.
Ved dette angreb er det *integriteten* og *fortroligheden* der påvirkes, da angriberen kan læse og ændre indstillinger på ICD'en.

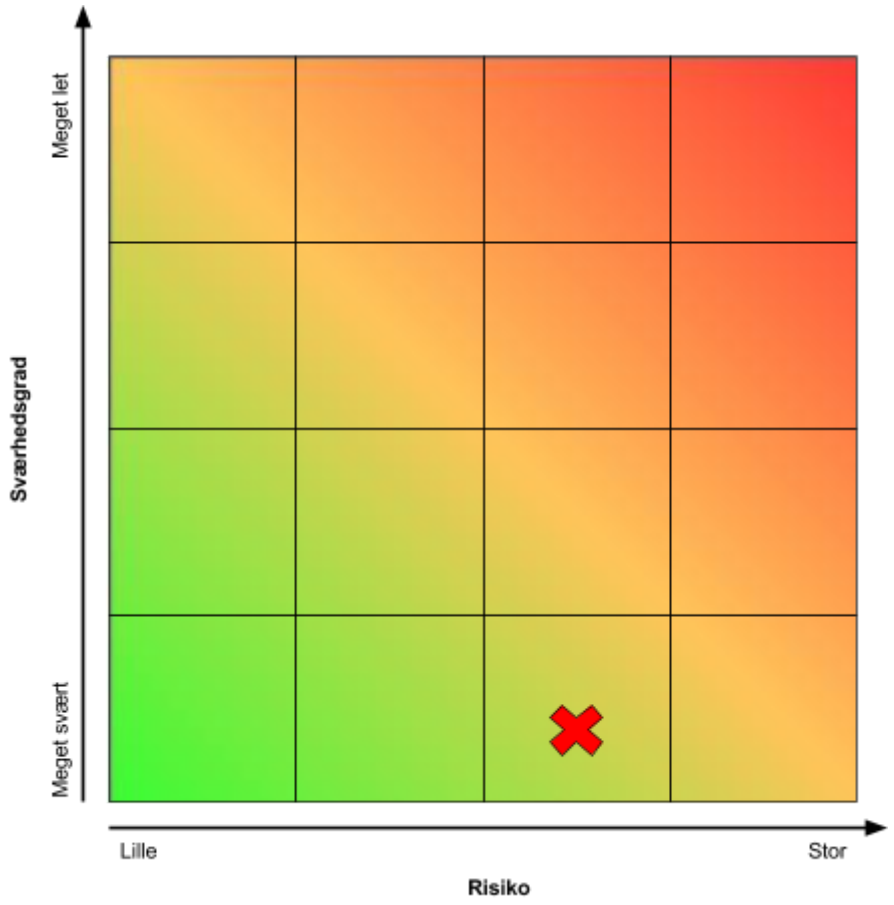


Figur 14: Graf - Stjæle universal aflæsningsudstyr

Dette angreb vil jeg sige er middelsvært at udføre, da der skal både noget social engineering til at få fingre i et sådant apparat fra et hospital samt lidt held. Det er dog set, at sådanne apparater har været til salg på eks. ebay.com. Ud over at skaffe udstyr, skal angriberen også kunne slæbe et stort apparat rundt, samtidig med at han uset kommer tæt på patienten. Hvis det udføres med succes vil risikoen være stor, men da sværhedsgraden er så høj, samt at der ikke rigtig er nogen gevinst for angriberen, placerer jeg krydset lige under middel i sværhedsgrad og lidt over middel som risiko.

8.1.7 Radiobølgeangreb

En angriber kan få en pacemaker til at tro, at hjertet slår forkert, ved at skyde med kraftige radiobølger mod pacemakerens sensor som sidder fast på hjertet.



Figur 14: Graf - Radiobølge angreb

Dette angreb er svært at udføre, og angriberen skal ret tæt på offeret, for at det skal kunne lykkedes. Risikoen er lidt over middel. De nyeste versioner af ICD-pacemakere er ret gode til at se forskel på ægte hjerterytme og støj fra omgivelserne. Derfor placeret krydset nede i det lysegrønne område.

8.2 Konklusion

Det var muligt at finde mange spændende angreb imod systemet, og flere af dem er nogle, jeg selv har tænkt over i hverdagen. Flere af de beskrevne angreb er allerede blevet bevist mulige at udføre [5] [8] [9] [10] [17] [18]. Dog har det taget rigtig lang tid for et helt team at udføre, og de har haft fuld adgang til den enhed, de forsøger at angribe. Det er endnu ikke noget, som alle og enhver bare kan downloade et program til, og så gå igang med at overtage naboens pacemaker eller ICD. Der er endnu ikke blevet registreret et angreb, hvor en patients pacemaker er blevet angrebet af en hacker. Én ting der går igen for graferne er, at angrebene er meget svære at udføre, og det forudliggende arbejde det vil tage at udvikle disse angreb ikke gør det særligt sandsynligt, at de overhovedet bliver et problem. Det er jo ikke et banksystem, hvor man kan stjæle penge. Dog kan man tænke sig, at en angriber kunne benytte et af disse angreb i et ransomwareangreb. Patienten får at vide at hans pacemaker er blevet angrebet, og hvis der ikke betales til angriberen, vil pacemakeren blive indstillet til en indstilling, som han måske vil dø af. Det kunne også bare være at pacemakeren slukkes indtil der er betalt. Dette er straks mere alvorligt, men igen er der stadig ikke set eksempler på denne type angreb.
Dog skal man være opmærksom på, at indenfor sikkerhed kan der pludselig opstå nye teknikker, trends eller måder at bryde systemer på, som kan ændre hele billedet. Derfor er det vigtigt, at hvert enkelt kendt angreb bliver taget alvorligt og løbende bliver genvurderet. Personligt frygter jeg ikke, at disse angreb vil ske mod netop min ICD-pacemaker.

9 Sikkerhed eller patientsikkerhed

Når vi taler om sikkerhed handler det om hvorvidt ens system som i dette tilfælde er et medicinsk apparat, bliver ramt på et af de tre dele fra FIT-modellen. Når vi taler patientsikkerhed er det selve patientens helbred, der bliver ramt ved et eventuelt angreb. Faktisk behøver det ikke at være et angreb, som rammer patientsikkerheden. En slem fejl i enten enhedens software eller i selve systemdesignet kan true patientsikkerheden. Indenfor medicinske apparater, som er indopereret i brugeren, har brugeren begrænset batterikapacitet til rådighed, og da der endnu ikke findes godkendte systemer, hvor det er muligt at genoplade batteriet, er genopladning ikke en mulighed.

En ICD-pacemaker som den, jeg i dag har indopereret, kan alt efter hvor meget, den har at lave, holde strøm i op til 10 til 12 år. Den første model jeg havde for snart 20 år siden, blev skiftet efter bare 7 år. Dette betyder, at så snart batteriet er brugt op, skal der en operation til, for at skifte batteriet. For enhver operation er der risiko for komplikationer og specielt for pacemakere kan det være infektioner, eller kroppen kan udstøde pacemakeren. Selv om alt går godt, vil patientens livskvalitet og hverdag blive udfordret i flere uger før og efter operationen. Alt dette går ud over patientsikkerheden og i værste fald kan patienten dø hvis pacemakeren løber tør for strøm. Enten af sygdommen, som gør, at man har brug for pacemakeren eller af komplikationer ved selve operationen.

Der skal spares så meget som muligt på batteriet i alt hvad der foretages i både kommunikation båndbredde og beregninger. Dette betyder, at kommunikation med apparatet skal være så minimalt som muligt, og der skal sendes så lidt som muligt frem og tilbage. Det skal også undgås, at der skal bruges energi på store beregninger, som vil bruge ekstra energi. Dette udelukker mange af de kendte sikkerhedsteknologier der bruges indenfor sikkerhed i dag. Her laves der store beregninger til at kryptere og dekryptere, og der kommunikeres frem og tilbage mange gange uden tanke på båndbredde eller CPU-forbrug. Man kan sige, at alt der gør, at patienten ikke kan få den behandling fra apparatet, som han har brug for, eller ting der gør, at der skal flere operationer til end normalt, går ud over patientsikkerheden.

10 Patientsikkerhedsmekanismer

I modsætning til de eksisterende kendte sikkerhedsmekanismer, der bruges i dag, findes der forskningsprojekter [6], som forsøger at opfinde nye sikkerhedsmekanismer, som vil kunne højne både sikkerhed, patientsikkerheden og batterilevetiden. Her vil jeg gennemgå både nogle af de gamle teknologier samt den nye forsknings eksempler, som måske en dag bliver standarden.

10.1 No Security

Der findes ældre modeller af pacemakere, hvor der nærmest ingen sikkerhed er indbygget i det trådløse interface. Dette er den mindste form for sikkerhed og giver hverken sikkerhed eller patientsikkerhed. Denne form anbefales absolut ikke til livsvigtige apparater såsom pacemaker og ICD'er.

10.2 Auditing

Hvis man indfører logning af alle vigtige funktioner, vil man kunne se, om der har været andre inde og ændre i enheden. Dette alene højner ikke patientsikkerheden men idet at man kan se, at der har været andre inde og lave uautoriserede ændringer, vil man kunne håndtere dette sikkerhedshul og måske i næste version have lidt bedre sikkerhed. Auditing kan også være et problem, da der er begrænset hukommelse og processorkraft til rådighed for at holde strømforbruget nede. Derfor skal det kun være det allermest vigtige som logges og samtidig skal loggen kunne nulstilles ved næste serviceeftersyn. Det er også en mulighed at logge til en ekstern hardwareenhed uden for kroppen, som så opsamler det trådløse signal og behandler logdataen. Dette vil hjælpe med begrænset pladsproblematikken, og man undgår at indbygge yderligere hukommelse i enheden. Hvis enheden skal have tilføjet mere hukommelse, vil det gøre den fysisk større, og dermed gå ud over patientsikkerheden. Dette fordi patienten skal gå rundt med en større indopereret enhed, hvilket er mere belastende for kroppen i form af nemmere afstødelse af fremmedlegemet og øget infektionsrisiko. Der findes flere eksempler på eksterne enheder, som allerede findes på markedet i dag blandt andet kan nævnes MedMon [7], som kan sættes op til at logge den trådløse trafik samt detektere anormaliteter.

10.3 Krypteringsmekanismer

Kryptering af den trådløse forbindelse mellem det medicinske apparat og aflæsningsenheden vil være en oplagt løsning til at undgå, at en angriber kan angribe og udnytte ens IMD. En fornuftigt krypteret kommunikation vil kunne nedsætte risikoen for, at et af de 3 punkter i FIT-modellen bliver angrebet. Men her er det medicinske apparater, vi har med og gøre, og det betyder, at der er andre problematikker, som så kommer i spil.

10.3.1 Public-nøgle

Et system bygget op omkring public key kryptering lyder i første omgang som en god ide til medicinske apparater, da der vil kunne opnås en krypteret forbindelse, hvor hver side har sin private nøgle til at læse beskeder og en delt public nøgle til at kryptere beskeder med. Dette fungerer desværre ikke i praksis, da de protokoller, der er bygget op omkring Public key kryptering i dag generelt bruger meget mere regnekraft og dermed også batteri. Det vil også kunne udnyttes, at der bruges algoritmer, som kræver meget regnekraft. Eksempelvis vil en angriber kunne udføre et denial of service angreb, hvor angriberen prøver at forbinde mange gange til enheden. Dette vil kunne dræne batteriet eller den begrænsede mængde tilgængelig regnekraft vil gå ud over enhedens mulighed for at gøre det arbejde, som den oprindeligt er sat til at lave, såsom at holde et menneske i live. Alt der kræver meget strøm som dette går ud over patientsikkerheden og er ikke optimalt for livsvigtige medicinske apparater.

10.3.2 Symmetrisk nøgle

Flere af de nyere ICD og almindelige pacemakere gør brug af symmetrisk nøgle kryptering hvilket vil sige, at begge sider kender en delt nøgle, som bruges til både at kryptere og dekryptere beskeder med. Denne fremgangsmåde er meget simpel at bruge og bruger ikke meget strøm. Det giver så desværre andre problemer, såsom hvor nøglerne skal gemmes og at hvis en angriber får fat på en nøgle, så er der fri adgang og nøglen kan ikke skiftes ud. Igen skal vi tænke på patientsikkerheden, da en patient skal kunne få sin behandling, når der er brug for den. Alle brugere som har en bestemt type enhed indopereret, skal have samme mulighed for at få den rette behandling, lige meget hvilket land de befinder sig i. Det vil sige, at selvom du er på ferie i Australien, skal det lokale sygehus kunne få adgang til

netop din enhed og lave de nødvendige aflæsninger eller indstillinger. Det kan være livstruende, hvis ikke det er muligt for hospitalet at få adgang til enheden. Der findes tusindvis af apparater på hospitaler rundt omkring i verden, som alle kan forbinde til hvilken som helst version af pacemakere. Så alle der kommer forbi og har brug for behandling kan få det. Det kunne tænkes, at det i nogle lande vil være lettere end i andre at få fat på et sådant apparat for en angriber. Men igen skal der tænkes på netop patientsikkerheden.

10.4 Nøgleopbevaring

Til kryptering er nøgledistribution altid det store problem. Her er et par eksempler på forslag hvordan man kan opbevare nøglen.

10.4.1 Halskæde

Man kan have en halskæde, som indeholder nøglen til at få adgang til at kommunikere med enheden. Det vil sige, at lægens aflæsningsudstyr ikke kan kommunikere medmindre patienten har husket at tage sin halskæde med. Dette er farlig metode, da man ved, at mennesker begår fejl og hvis halskæden bliver væk vil det ikke længere være muligt at kommunikere med pacemakeren, og så skal der igen en operation til, da hele enheden skal skiftes ud.

10.4.2 Tatovering

Et andet forslag har været, at patientens nøgle kunne blive tatoveret på patientens hud med ultraviolet blæk, så patienten altid har sin nøgle ved hånden. I dette eksempel skal lægen scanne patientens tatovering for at få adgang. Dette kan også udnyttes af en angriber som kan læse koden med uv lys og senere udnytte det til et angreb. Igen kan nøglen blive væk, eller med tiden blive ulæselig.

10.5 Cloaker

Dette er et forslag om en halskæde, som løbende snakker med patientens IMD. Når den kan se, at cloakeren er i nærheden, slukker den for alt kommunikation i et vist stykke tid. Næste

gang der forbindes, vurderes der igen om cloakeren er i nærheden, og om der igen skal åbnes for muligheden for at kommunikere med pacemakeren. Dette scenario vil gøre, at så længe man har sin halskæde på ude i verden, vil der ikke kunne kommunikeres via den trådløse forbindelse. Det er igen et problem at hvis halskæden bliver væk, er man ikke længere beskyttet.

10.6 Startknap

Et forslag af den lidt mere bizarre slags er, om en knap der indopereres i patienten under huden, som der fysisk skal trykkes på, inden der kan oprettes trådløs forbindelse til pacemakeren. Her er det meningen at lægen skal trykke på knappen, inden der oprettes forbindelse. Det er ikke, alle der vil blive glade for, at de pludselig skal have ekstra hardware indopereret, og dette går ud over patientsikkerheden, da mere hardware i kroppen giver flere bivirkninger. Der er også større risiko for hardwarefejl, hvis knappen f.eks sætter sig fast, og en angriber dermed altid kan få adgang.

10.7 Biometrics

Her skal der tages biometric information om patienten, som lægges i pacemakeren allerede inden den bliver indopereret. Dette vil gøre, at patienten skal scannes inden der oprettes forbindelse. Det kan være patientens øje eller fingeraftryk som lægen scanner, før der kan oprettes forbindes. Dette kan være farligt, da der stadig er meget usikkerhed i de biometrics former vi har i dag, og over tid kan disse værdier ændre sig. Hvad nu hvis fingeren falder af eller øjet bliver beskadiget så skal der en stor operation til for at skifte pacemakeren. Dette vil gå ud over patientsikkerheden.

10.8 Anomaly detection

Et stort problem er, at det ved mange af disse teknologier stadig er muligt for en angriber at udføre et denial of service attack ved at lave mange gentagne forespørgsler til enheden og med tiden opbruge alt enhedens strøm. Dette kan medføre at i stedet for at holde strøm i 10 år kan den nu kun holde strøm et par uger. Til at undgå eller begrænse dette, kan anormalitets-detektering bruges. Dette gøres ved at forskellige regler opsættes i enheden,

således at hvis en af disse regler bliver brudt, sættes en alarm i gang. Et eksempel kan være hvor meget strømforbrug der maks må være registreret indenfor et døgn. Alarmen kan så være en fysisk alarm ved at enheden giver en høj lyd, som betyder, at patienten skal kontakte hospitalet, eller det kan være, at hjemmemonitoreringen sender alarmen med til hospitalet ved den natlige logning. Der findes flere forskellige måder at gøre dette på men, essensen af det hele er, at hospitalets eksperter hurtigst muligt skal informeres om anormaliteterne, så disse kan stoppes.

10.9 BTG policies

Breaking The Glass policies betyder at brugere i en kritisk situation skal have adgang til mere, end de normalt har. Dette vil selvfølgelig i den kritiske periode give nemmere adgang for en angriber, men det er patientsikkerheden, der er vigtigst. Det er må prioriteres vigtigere, at sygeplejersken på det lokale hospital eller ambulancelægen kan ændre på livsvigtige indstillinger, de normalt ikke har adgang til, end at en angriber ikke får lidt lettere ved at lave et angreb lige i den kritiske periode. Ved denne type beskyttelse er det vigtigt, at når status for det medicinske apparat igen er tilbage i normal operations mode, skal de ekstra rettigheder igen sættes tilbage til standard.

Subject	Role	Operation	Object	BTG	Obligations
Doctor	r^1	read	ob^1	-	oblg [Write to Audit]
Doctor	r^2	read	ob^2	-	-
Nurse	r^3	read	ob^1	BTG	-
Nurse	r^3	$O^{BTG(read)}$	ob^1	-	oblg [Notify Manager; Write to Audit; Trigger the alarm]
Nurse	r^4	read	ob^2	-	oblg [Write to Audit]
Staff	r^5	read	ob^2	BTG	-
Staff	r^5	$O^{BTG(read)}$	ob^2	-	oblg [Notify Manager; Write to Audit; Trigger the alarm]

Figur 15: Tabel - BTG Policies

http://researchprofiles.herts.ac.uk/portal/files/7807268/1569953163.pdf

Figur 15 viser et eksempel for break the glass policies designet til et patientdatasystem. Noget af det samme kunne tænkes for medicinske apparater, hvor man får rettigheder til at ændre indstillinger på enheden i stedet for læse- og skriverettigheder til patientjournaler - som i dette eksempel. Diagrammet ovenfor har 5 forskellige roller fordelt på 3 subjecter; doctor, nurse og staff. Alt efter hvad sikkerhedsniveauet er for det objekt der skal læses, kan der forekomme forskellige obligations. Eksempelvis bliver det skrevet i audit-loggen, hvis lægen læser et object af type ob1, hvorimod hvis lægen læser et object af type ob2, bliver der ikke logget noget. Man kan se at Sygeplejersken godt kan læse objekter af typen ob1 men det kræver at BTG-tilstanden aktiveres, hvilket gør, at en manager bliver notificeret herom, og der aktiveres en alarm. Dette system kræver meget opsætning og vedligeholdelse at holde kørende og en enkelt fejlopsætning kan have store konsekvenser. Tidligere medarbejdere skal fjernes fra systemet, og nye skal tilføjes. Samtidig skal man have disciplin til, at alle alarmer og auditlogs tages alvorligt og bliver vurderet fra gang til gang. Et sådant system kan hurtigt drukne i alarmer, og hvis der kommer falske alarmer hver dag, vil de til sidst ikke blive taget alvorligt. Et sådant system kan også udnyttes af en angriber, som med social engineering, fishing eller simpel passwordgætteri kan være heldig at kunne få adgang til systemet. Selvom det kun lykkedes ved en bruger med mindre rettigheder, vil det stadig kunne udføre kritiske funktioner da BTG kan aktiveres. Det er ikke sikkert, at det er alle brugere som har lige stor viden om sikkerhed. Hvis en af disse brugere kan få adgang til

kritiske funktioner ved et tryk på en knap, der popper op, kan det være for sent at gøre noget ved det når først skaden er sket..

10.10 Oversigt

Measure		Type	Safety	Security	Battery Life	Security Properties Addressed
No security		*	–	–	*	None
Auditing		Detection	–	–	+	Non-Repudiation
Cryptographic Measures		Protection	–	+	±	Authentication, Confidentiality, Integrity
AC	Certificates & Lists	Protection	–	+	±	Authorization (+Authentication)
	External Devices	Protection	+	±	+	
	Internal Devices	Protection	+	+	*	
	Proximity	Protection	+	±	*	
	Biometrics	Protection	+	+	*	
Anomaly Detection		Protection	–	+	+	Authorization, Availability
BTG Policies		Protection	+	–	*	Authorization during emergencies

*Legend: + Positive; – Negative; ± Both positive and negative effects; * No influence.*

Figur 16: Tabel - Patientsikkerhedsmekanismer

C. Camara et al. / Journal of Biomedical Informatics 55 (2015)

På figur 16 ses en oversigt over, hvilke af de omtalte sikkerhedsmekanismer, der opfylder henholdsvis patientsikkerheden, sikkerhed og batterilevetid. Dette er en fin oversigt, men man skal holde sig for øje, at mange af de omtalte teknikker stadig er i designstadiet og der kan gå mange år, før det er testet og godkendt til at blive brugt i den virkelige verden. Det skal også nævnes, at patienter, der har ældre model pacemaker generelt ikke bliver opereret, bare fordi der kommer en ny opgraderet version. Man venter normalt til, at der ikke er mere strøm på den de har, og så ser man, om der er en nyere godkendt model, når den gamle alligevel skal skiftes.

10.11 Konklusion

Alt i alt er der mange spændende forslag til hvordan, patientsikkerhed, sikkerhed og batterilevetid opretholdes. Der er dog ikke nogen af dem som er uden konsekvenser og jeg tror det er derfor, der endnu ikke er kommet en standard. Det er spændende at se, hvad fremtiden bringer og hvad der bliver fremtidens standard. Personligt synes jeg, at det er vigtigt, at patienterne også tages med på råd om, hvilken model og hvilke funktionaliteter der bliver aktiveret i netop den model patienten får tilbudt.

10.11.1 Min erfaring

Når jeg ser tilbage på min egen historie med både gamle og nye pacemakere de sidste 20 år, ville jeg gerne have været bedre informeret om hvad min ny ICD-pacemaker kunne, da jeg ved batteriskift blev opgraderet til en nyere version med mulighed for hjemmemonitorering. Blandt andet ville jeg gerne have været informeret om, at jeg nu havde et trådløst interface direkte til mit hjerte og om hvilke natlige informationer, der bliver sendt om mig samt hvem der har adgang til disse informationer. Jeg har også haft en episode, hvor jeg skulle sælge en 12” subwoofer på Den Blå Avis. Da jeg skulle bære højtaleren ud til bilen, kom den for tæt på min pacemaker hvilket startede en høj hyletone, som varede ved i ca. 30 sekunder. Dette gjorde, at jeg gik i panik og troede, at jeg skulle have et kraftigt stød som er det, ICD-pacemakeren er sat i for at gøre, når hjerterytmen er for hurtig. Heldigvis viste det sig, at den nye model blot havde en funktionalitet som gjorde, at hvis den blev udsat for et kraftigt magnetfelt, slukkede den automatisk, indtil den igen var uden for magnetfeltet. Der var så aktiveret i indstillingerne, at der skulle komme en alarm, når dette skete. Denne alarm var den høje hyletone. Det ville have været rart at vide inden det skete, og eventuelt have mulighed for at vælge, at slå alarmen fra..

11 Udvikling af medicinske apparater

Der bliver i dag opfundet og videreudviklet smarte medicinske apparater som kan forlænge og forbedre menneskers liv. Alt dette er meget godt, og kan gøre hverdagen nemmere for rigtig mange mennesker. I fremtiden kan vi næsten kun gætte på, at det bliver endnu mere normalt, at sygdomme helbredes ved hjælp af diverse indopererede løsninger. Det kan være en skræmmende tanke, at software er ansvarligt for menneskeliv, men på den anden side er det jo godt, at man kan forbedre og forlænge patienters liv.
FDA Food and Drug Administration i USA har udviklet en guideline [11] [18] til, hvordan de mener, at man bedst muligt udvikler medicinske apparater med fokus på sikkerhed. Jeg vil beskrive hvad FDA's guideline overordnet går ud på og sammenligne den med three pillars of software security [2] [4], som er den guideline vi har lært om i løbet af masterundervisningen.

11.1 FDA premarket guideline

I 2014 udgav FDA en premarket guideline med anbefalinger til udvikling af medicinske apparater med fokus på sikkerhed.
Premarket er tiden inden apparatet er blevet godkendt og frigivet til salg på markedet. Det anbefales her, at der allerede tænkes på sikkerhed fra den tidlige designfase til og med valideringfasen inden systemet kommer på markedet. Trusler og svagheder skal identificeres og der skal beskrives, hvor stor indvirkning de forskellige trusler har på apparatets funktionalitet og evne til at udføre det arbejde, den er sat til at gøre.
Der skal også vurderes hvor sandsynligt det er, at hver trussel bliver udnyttet samt udarbejdes en strategi for, hvordan den bliver afværget eller minimeret.
Det anbefales, at der i udviklingsprocessen benyttes NIST-sikkerhedsframework. Dette framework består af en række værktøjer som kan benyttes under udvikling af systemet og kan gøre systemet mere modstandsdygtigt mod eventuelle angreb.
NIST består af 5 hovedpunkter *identificere*, *beskytte*, *detektere*, *reagere* og *genskabe* som skal indtænkes i systemløsningen. Under hvert hovedpunkt er der flere eksempler på løsninger, som kan vælges alt efter behov og ambitioner.

11.1.1 Identificere

Identificere handler om at få fundet eventuelle trusler, mod systemet og få dem håndteret. Her er det også vigtigt at få det gjort synligt for organisationen hvilke udfordringer der er, så der kan planlægges og afsættes de rette ressourcer.

11.1.2 Beskytte

Systemet skal designes så det er muligt at beskytte de mest kritiske funktioner mod eventuelle angreb. Hvis et angreb alligevel sker, skal de kritiske funktioner stadig kunne virke. Det kan som i denne rapport handle om livsnødvendig behandling. Angrebets indvirkning skal håndteres så eventuel skade mod systemet mindskes. Måske er det ok at hjemmemonitoreringen ikke virker under angreb, men den livsnødvendige pacemakerbehandling skal altid køre videre ligemeget om der er et angreb i gang.

11.1.3 Detektere

Systemet skal designes til at kunne detektere, når der er et angreb i gang. Ved tidligt at kunne se, at et angreb er i gang, kan skaderne begrænses og der kan lukkes ned for mindre kritiske områder.

11.1.4 Reagere

Når systemet ved, at der er et angreb i gang, skal det også reagere herpå. Dette punkt indeholder alle de special cases der skal ske, når forskellige typer angreb sker.

11.1.5 Genskabe

Der skal implementeres funktionalitet som kan genskabe systemet til sin oprindelige normaltilstand når et eventuelt angreb er ovre. Beskadigede dele skal genskabes og fuld funktionalitet skal igen aktiveres.

11.2 FDA Post Market principper

Da det ikke er alle sikkerhedstrusler man kan forudse ved at have en fornuftig premarket process udgav FDA i 2016 en post market guideline som beskriver, hvad de anbefaler af processer for at opnå bedre sikkerhed efter udgivning og markedsintroduktion af produktet.

11.2.1 ISAO

FDA ser sikkerhedstrusler mod medicinske apparater som en fælles kamp, der går helt fra hardware producenterne via sygehuset og helt ud til patienterne. I fællesskab opnås der bedre mulighed for at opdage eventuelle angreb og rapportere dem samt få dem elimineret. Det anbefales, at producenter af medicinske apparater taler sammen i såkaldte ISAO fællesskaber hvor der deles viden og erfaringer. ISAO står for information sharing analysis organizations.

11.2.2 Risk management

Det anbefales at der laves processer for risikohåndtering som gennem hele produktets levetid løbende opdateres og revurderes. Alle kendte angreb mod systemet dokumenteres, evalueres og håndteres. Hele risikovurderingsprocessen skal være en gentagende proces, som over tid opdager og håndterer nye trusler. FDA anbefaler, at trusler vurderes på to punkter.

1) Sværhedsgraden af angrebet.
2) Graden af patientskade, hvis angrebet skulle ske.

11.2.2.1 Common Vulnerability Scoring System

Figur 17: Web - Common vulnerability scoring system

https://www.first.org/cvss/calculator/3.0

FDA anbefaler også, at man bruger et rating tool til at hjælpe med at udregne en score for sværhedsgraden af de enkelte angreb, der bliver fundet i risikovurderingsprocessen. Et sådant tool kan hjælpe med bedre ensartede vurderinger, så man nemmere kan se, om det er et kritisk angreb, hvor der skal tages action hurtigst muligt. FDA nævner Common Vulnerability Scoring System [20] som er et værktøj der giver en score høj, medium eller lav ud fra informationer om angrebet.
På billedet ses de enkelte punkter, som man skal vælge et svar til, og når alle punkter er besvarede får man en score. Dette er en nem måde at få en score på uden at man behøver at være en garvet sikkerhedsekspert.

11.2.2.2 Patientsikkerhed

Figur 18: Graf - FDA severity of patient harm
https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

Når vi har de to værdier for en trussel, kan de sættes ind på en graf som den på billedet ovenfor. Dette kan så bruges til at se hvilke trusler, der skal tages hånd om. De kontrollerede trusler kan godt accepteres i et system, hvorimod de ukontrollerede ikke kan. Hvis der opstår en ukontrolleret trussel, skal der gøres noget for at løse den, og dette bringer os videre til næste punkt, som er rapportering og firmware opdateringer.

11.2.3 Rapportering

Når der i risikovurderingen dukker en ukontrolleret trussel op er det vigtigt at få den kontrolleret hurtigst muligt. Dette kan være svært, når det er et produkt, som allerede er på markedet og indopereret i patienter over hele verden. Fra premarket guiden kan vi huske, at det er blevet anbefalet, at systemet blev designet med mulighed for firmware updates. Dette vil være en god måde at håndtere nyopdagede ukontrollerede trusler. FDA opfordrer fabrikanter til at indrapportere deres fund til den ISAO gruppe de er medlem af, og udstede en plan for firmwareudrulning som fikser problemet. Ved firmwareopdateringer og patches

som retter sikkerhedsbrister i et system, vil det ikke kræve godkendelse fra FDA som det gør, når man første gang skal have et produkt godkendt hos FDA. Dette kan være med til at sikkerhedsopdateringer kommer hurtigere på markedet end normale rettelser.

11.3 FDA vs three Pillars

FDA [11] [18] og three Pillars of Software Security [2] [4], som jeg brugte til at analysere ICD-pacemakeren i tidligere afsnit, har mange af de samme generelle anbefalinger om, hvordan man udvikler systemer med fokus på sikkerheden. De to minder utroligt meget om hinanden og lige meget hvilken man vælger at følge, vil det være en stor forbedring af sikkerheden i modsætning til, hvis man slet ikke gøre noget. Der findes i begge guidelines en række anbefalinger til aktiviteter som kan benyttes i udviklingsforløbet til at opnå bedre sikkerhed i de enkelte faser. Risikohåndtering er i begge guidelines en grundlæggende gentagende aktivitet som på en let og overskuelig måde kan bruges til at vise organisationen, hvor det er vigtigt, at der bruges ressourcer for at forbedre sikkerheden. FDA anbefaler at man deltager i såkaldte ISAO “Information Sharing Analysis Organisations” grupper for at dele sin viden med andre indenfor samme felt. Det minder utroligt meget om three pillars of software securitys tredje søjle “Knowledge” som også går ud på at dele og opsamle viden. For begge handler det om at få delt sin viden med andre og blive inspireret samt lære af andres viden og erfaringer indenfor sikkerhed. Hvis jeg skulle vælge én af de to til at udvikle medicinske apparater som ICD-pacemakeren, ville jeg vælge FDA, da den er designet specifikt til medicinske apparater. I guiden bliver der taget højde for både pre- og post market aktiviteter, så man også følger apparatet efter det er sat i produktion. Pre market anbefaler en løsning, hvor der er mulighed for, at firmwareopdatere sin enhed og dermed håndtere sikkerhedstrusler som findes efter apparatet er sat i produktion. Dette gør FDA til mit førstevalg. En anden god ting i FDA’s guidelines er at, de har beskrevet en række værktøjer, som kan være med til at gøre det nemt og overskueligt at implementere de enkelte aktiviteter i sin udviklingsproces. Jeg er selv tilhænger af værktøjer, som gør ens arbejdsgang nemmere. Hvorfor designe noget selv, som andre har gjort nemt for dig? Et andet punkt, som jeg godt kan lide ved FDA, er deres anbefaling om at softwaresystemer i medicinske apparater skal kunne detektere, når der er et angreb i gang. Når systemet ved, at det er under angreb, kan det slukke for nogle af sine funktioner og undgå, at de bliver udnyttet og stadig køre videre i kritisk tilstand, så patienter stadig får deres livsvigtige behandling. Den tankegang passer perfekt på livsvigtige medicinske apparater som ICD-pacemakeren.

12 Konklusion

Jeg er blevet klogere på sikkerheden omkring min ICD-pacemaker, og har fået åbnet øjnene op for, at der måske ikke er helt så meget sikkerhed indbygget, som jeg troede. Det har specielt været meget spændende at blive klogere på de problemstillinger, der findes mellem sikkerhed og patientsikkerheden, hvor man ikke kan bruge ubegrænset strøm og regnekraft. Dette giver god mening, når jeg tænker tilbage på min egen historie med sygehusvæsenet, hvor jeg ikke selv har fået noget at vide når de har indført nye potientielle angrebsflader direkte til mit hjerte. De står på den side hvor der tænkes patientsikkerhed og det vigtigste er, at jeg får min behandling.

Det er godt at se, at der tænkes i nye metoder til at opretholde både sikkerhed og patientsikkerhed og det bliver meget spændende at se, hvad de nye modeller kommer til at indeholde i fremtiden, og om der bliver bedre information til patienterne. Sikkerhedsanalysen jeg lavede, giver et godt billede af at der overordnet kan være flere steder som pacemakeren kan angribes på, men at de alle er ret besværlige at udføre, da der skal bruges meget tid, penge og kræfter på at skaffe det rette udstyr. Samtidig skal man også være indenfor kort rækkevidde af den pacemaker man vil angribe for at det kan lykkes. Inden projektet havde jeg en tanke om, at software og hardware i min pacemaker var fuldstændig sikkert, og at det var propfyldt med sikkerhedsmekanismer så det ville være umuligt at bryde ind i den. Dette har jeg efterfølgende fået et andet syn på. Ikke at jeg er blevet mere bange for, at der vil ske noget med min ICD. Jeg mener, at hvis man vil afpresse mig, så findes der andre nemmere og billigere måder at gøre det på. Det er rart at se, at en guideline som FDA's er af så høj kvalitet og jeg mener, at det er et skridt i den rigtige retning til bedre sikkerhed i medicinske apparater, som f.eks min ICD.

I løbet af mit masterforløb har jeg fået et godt indblik i generelle sikkerhedsproblematikker samt lært teknikker og metoder til at udvikle og analysere software med fokus på sikkerheden. Jeg har lært at tænke sikkerhed og indset, at sikkerhed ikke er noget, man bare implementerer på et antal timer, og så er ens system 100 % sikkert resten af dets levetid. Sikkerhed er en proces hvor der hele tiden revurderes og analyseres for at finde nye sikkerhedstrusler mod systemet, som skal håndteres bedst muligt. Dette kan være svært at forklare til resten af ens organisation, og vi kender alle det med, at udviklerne selv kender de steder, hvor sikkerheden i systemet ikke er optimal.

Der er ikke altid tid og penge til at få lov til at gøre noget ved de kendte trusler. Hertil har vi lært, at en simpel og overskuelig sikkerhedsvurdering er et godt værktøj, som kan benyttes til at vise ledelsen hvilke sikkerhedsopgaver det ville være smart at håndtere først, og på den måde få bevilling til at implementere rettelserne.
Alt i alt har det været et meget lærerigt masterforløb med masser af ny viden samt redskaber, jeg kan tage med mig videre i mit daglige arbejde som softwareudvikler. Jeg vil klart anbefale andre udviklere, som ønsker at forbedre sig, til at tilmelde sig masteruddannelsen.

13 Referencer

[1] https://groups.csail.mit.edu/netmit/IMDShield/ - billede forside

[2] Gary McGraw - Software security Building software

[3] http://www.heartrhythmspecialistsla.com/services-transtelphonic-monitoring-los-angeles-ca.html - Transtelephonic forklaring

[4] http://www.swsec.com/resources/pillars/ - the three pillars of software security

[5] https://www.theregister.co.uk/2016/01/05/researcher_hacks_her_own_pacemaker/ - Marie Moe artikkel

[6] http://www.seg.inf.uc3m.es/~jet/papers/2015jbi.pdf - C. Camara et al. / Journal of Biomedical Informatics 55 (2015) - nye sikkerhedsmekanismer

[7] https://www.ncbi.nlm.nih.gov/pubmed/24473551 - MedMon

[8] http://scholarworks.umass.edu/cgi/viewcontent.cgi?article=1067&context=cs_faculty_pubs - ICD-pacemaker radio angreb

[9] https://www.rt.com/usa/hacker-pacemaker-barnaby-jack-639/ - Barnaby Jack artikkel

[10] http://sciencenordic.com/researcher-discovered-her-pacemaker-hackable - Marie Moe artikkel

[11] http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf - FDA Post market guideline

[12] http://dl.acm.org/citation.cfm?id=2507771.2508701 - Controlling for cybersecurity risks of medical device software

[13] http://cacm.acm.org/magazines/2016/10/207766-a-brief-chronology-of-medical-device-security/fulltext - Pacemakerens fejl historie

[14] https://www.wired.com/2016/03/go-ahead-hackers-break-heart/ - Marie Moe

[15] http://www.zdnet.com/article/data-from-pacemaker-used-to-arrest-man-for-arson-insurance-fraud/ - Pacemaker data brugt som bevis i retten

[16] http://researchprofiles.herts.ac.uk/portal/files/7807268/1569953163.pdf

[17] https://arstechnica.com/information-technology/2017/05/radio-controlled-pacemakers-arent-as-hard-to-hack-as-you-may-think/ - Hack pacemaker artikkel

[18] https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm356190.pdf - FDA pre market guideline

[19] http://blog.whitescope.io/2017/05/understanding-pacemaker-systems.html - 8000 vulnerabilities fundet i aflæsningsenhedder

[20] https://www.first.org/cvss/ - common vulnerability scoring system

[21] https://youtu.be/d3P6fvKWLiE - ICS Security Summit 2016:

[22] https://www.dr.dk/nyheder/viden/naturvidenskab/er-det-farligt-naar-hjertet-er-paa-internettet - Hack pacemaker artikkel dr.dk

[23] http://www.theregister.co.uk/2010/07/29/cell_phone_snooping/ - GSM hacking

[24] https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update - FDA recall 500.000 Pacemakers