Blogpost monitoringsapparaten voor het meten van glucose waardes

Verdieping ICT | Joas van Bakel 2154346

Mensen met diabetes moeten een paar keer per dag bloedprikken, dit om de glucosewaardes te meten in het bloed. Daarbij is het nodig om ook een paar keer per dag insuline bij te prikken zodat de glucosewaardes op een veilig niveau blijven. In de afgelopen jaren zijn er veel ontwikkelingen gedaan op het gebied van de zorg, en hebben IoT (Internet of Things) apparaten al redelijk een plaats gekregen binnen de zorg. Zo zijn er draagbare monitoringsapparaten die naast glucose metingen ook insuline kunnen toedienen aan de drager van zo een apparaat. De beveiliging hiervan en dus ook de integriteit van data is bij deze apparaten van groot belang. Zodra deze niet kunnen worden gewaarborgd is het apparaat eigenlijk niet veilig te gebruiken. Dit aspect brengt eigenlijk alleen maar een nadeel voor technologische ontwikkelingen wat betreft de zorg. Zo zijn deze monitoringsapparaten die bijna geheel automatisch werken, en misschien wel beter als de mens zelf, nog niet zo veel gebruikt. De uitdading zit hem er namelijk in om de garantie te kunnen geven dat deze nieuw ontwikkelde methodieken dusdanig wel veilig genoeg zijn om te gebruiken. De uiteindelijk uitkomst mocht het wel goed fout gaan zou verre van de gewenste situatie zijn. Het idee van deze innovaties is namelijk om een aspect te verbeteren of makkelijker te maken. De voordelen van dit soort IoT apparaten is dat ze gemakkelijk inzichten kunnen geven en kunnen bepalen wat wel en of niet gedaan moet worden. Het grote nadeel van de apparaten is dat ze over het internet moeten communiceren. En zoals we weten is het internet geen veilig plek. De vraag die hier onder andere bijkomt kijken is: hoe wordt de integriteit bewaart tussen monitoringsapparaten en een partij van derden? (bijvoorbeeld een eventuele app).



Dit geeft mogelijkheden om op afstand de monitoringapparaten aan te vallen en uiteindelijk kwaadwillende acties uit te voeren (Senrio, 2017).

Om dit te voorkomen zijn er een paar voor de hand liggende maatregelen die we kunnen nemen:

1. Het minimaliseren van de communicatie;
2. Het vastleggen van buitenstaande verbindingen naar het apparaat toe
3. Het beveiligen van de lokalen opslag.

Het eerste aspect is het meest voor zichzelf sprekend, als we zo veel mogelijk communicatie minimaliseren, bestaat er ook een kleinere kans dat dit onderschept zou kunnen worden en verandert en daar de integriteit ten kosten van gaat. Maar uiteindelijk blijft deze communicatie het belangrijkst en moet deze blijven bestaan. Het is hierbij belangrijk dat binnenkomende verbindingen worden bijgehouden, met bijvoorbeeld logging. Hier kan men dan bijvoorbeeld ook een whitelist[[1]](#footnote-1) op toevoegen dat alleen geautoriseerde services verbindingen kunnen maken met de verschillende apparaten. Buitenstaande ‘vreemde’ verbindingen zullen dan niet geaccepteerd worden. Het derde punt wat hierbij erg van belang is dat de lokale opslag die gebruikt wordt door het apparaat ook daadwerkelijk beveiligd wordt, zodat aanpassingen aan bijvoorbeeld de whitelist niet mogelijk worden gemaakt.

Een nog niet genoemd aspect maar zeker ook belangrijk is dat veel IoT apparaten ook nog de mogelijkheid bieden om via een remote shell in te kunnen loggen. Dit principe is onder andere een bijkomst van het besturingssysteem waar het apparaat op draait, vaak is dit Linux. Hierbij worden jammer genoeg vaak standaard wachtwoorden gebruikt waarbij het kraken voor een aanvaller een stuk gemakkelijker wordt gemaakt. Fabrikanten zouden deze mogelijkheden moeten afschermen, omdat het simpelweg geen meerwaarde biedt voor de functionele eisen (Senrio, 2017).

Verder wordt geprobeerd de integriteit te waarborgen tussen partijen van derden door middel van kleine persoonlijke netwerken. Stel de volgende situatie voor, het monitoringsapparaat heeft een meting gedaan en gaat vervolgens data versturen naar de eindgebruiker. Deze gebruiker heeft een app waar de data uiteindelijk naartoe moet. Vaak wordt er dan gebruikt gemaakt van erg kleine draadloze persoonlijke netwerken. Dit betekent dat het bereik van het netwerk erg beperkt blijft. Een voorbeeld hiervan is een: low powered wireless personal area network (6LoWPAN). 3G, LTE en Bluetooth zijn andere voorbeelden van persoonlijke netwerken. Het voordeel van deze netwerken is dat een aanvaller fysiek erg dichtbij moet zijn om een aanval te realiseren. We moeten in gedachte houden dat dit soort apparaten niet erg krachtig zijn en dus niet goed kunnen werken met versleuteling. Daarbij hebben ze ook een minimale batterijduur, en deze energie moet zo efficient mogelijk worden gebruikt. Een mobiel apparaat daarentegen, heeft deze nadelen niet en is veel en vele mate krachtiger en kan in wezen dus wel de load aan die het versleutelen met zich mee brengt (Ahmed A. Mawgoud). Door het gebruiken van de kleine draadloze netwerken verminderen we de kans dat integriteit verloren gaat, maar elimineren hem niet volledig.

Naast integriteit moet de monitoringsapparaten bovenal veilig zijn, daarom kijken we wat de beste beveiligingsmethodieken er zijn om dit te kunnen realiseren. Er wordt gekeken naar de onderste methodes:

1. Encryptie
2. Autorisatie
3. RFID Authenticatie
4. Monitoring

Allereerst moeten we kijken naar wat de beste criteria zijn om antwoord te kunnen geven op de vraag welke het beste is. Binnen beveiligingsmethodes zijn er talloze principes die kunnen worden nageleefd. Deze principes dekken op zichzelf bijna alle kaders af die rond beveiliging een rol spelen. Met medische apparaten zijn dit er eigenlijk te veel om mee in te nemen in deze analyse (Somayeh Nasiri, 2019), daarom is er een selectie gemaakt uit de ‘belangrijkste’ van deze principes:

*De CIA-principes:*

1. Confidentiality  
   Het is erg van belang dat gegevens die worden overgezonden van sensor, naar telefoon en van telefoon, dat deze ten alle tijden confidentieel blijven. Dit omdat het erg privacygevoelige medische data is en niet zomaar ingezien mag worden. Dit ook mede bepaalt door regel- en wetgeving (bijvoorbeeld de AVG).
2. Integrity

Er moet een garantie zijn dat de data die uiteindelijk verstuurd wel integer is, omdat dit soort monitoringsapparaten een zeer belangrijke rol spelen bij het toedienen van insuline. Aan de hand van de geven informatie moet de eindgebruiker uiteindelijk een hoeveelheid insuline toedienen, en bij een verkeerde dosering kan het goed mis gaan.

1. Availability

Een ander zeer belangrijk aspect is dat de apparaten altijd beschikbaar moeten zijn, anders zouden bloedwaardes niet gemeten kunnen worden wat ook weer zeer nare gevolgen van dien heeft.

*En daarbij nog andere twee belangrijke aspecten:*

1. Reliability

Net zoals dat het apparaat goed beschikbaar moet zijn moet het apparaat ook over een bepaalde robuustheid beschikken. Het kan natuurlijk niet zo zijn dat het apparaat aan de hand van buiten liggende factoren niet of onvoldoende functioneert.

1. Accountability

Er moet een soort logging plaatsvinden zodat er nagekeken kan worden wie, en hoe het uiteindelijk is gegaan. Mede door dit punt hebben we dan ook een schakel in het systeem die we kunnen aanspreken als het een keer fout gaat.

*Beveiligingsmethodieken:*

Encryptie zorgt in weze wel voor veel betrouwbaarheid. Maar garandeert echter niet integriteit. Sommige protocollen die voor encryptie gebruikt kunnen worden kunnen dit wel, maar dit zorgt voor best wel veel overhead. Het probleem hiermee is dat de IoT apparaten maar een beperkte opslag en rekenvermogen hebben wat in weze weer de availibility vermindert. Autorisatie door middel van wachtwoordgebruik. Er moeten natuurlijk wel dingen gedaan worden met autorisatie. Hierbij is he van belang dat er nog bijvoorbeeld een controleslag wordt gemaakt naar de eindgebruiker toe. Het apparaat berekent bijvoorbeeld een waarde voor de insuline en daarbij moet de eindgebruiker dus toestemming geven om het toe te dienen. Het probleem hiermee is dat we weer een onafhankelijkheid creeeren naar een apparaat.

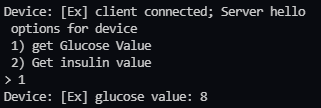
Zoals eerder gesproken gebruiken IoT devices vaak linux, maar laten hier de standaardwachtwoorden voor staan. Dit maakt het voor aanvallers wel gemakkelijk om bijvoorbeeld een backdoor aanval te realiseren. RFID Authenticatie. We kunnen door middel van een NFC chip in een mobiele telefoon authenticatie toevoegen. Hiermee weet het apparaat dan dat het mobiele device als legitiem wordt beschouwd en hiermee dus veilig mee kan communiceren. Daarbij is een telefoon al een persoonlijk apparaat en een aanvaller zou hiervoor dus wel fysiek aanwezig moeten zijn voor dat hij of zij in staat is om de authenticatie mogelijk te maken. (Heeft ook een beetje betrekking op de whitelist) i.c.m. met een fingerprint en of wachtwoord op de telefoon zelf maakt een goede beveiligingsmethodiek. Monitoring, zoals al eerder gezegd is het bijhouden van logs essentieel om vaak ook juridische aspecten af te dekken (denk hierbij aan non-repudiation). Het is dus ook van belang dat dit deel wordt afgedekt. Draagt in weze niet zo bij aan de betrouwbaarheid. Wel aan de integriteit betreffende de apparaat zijde. Accountibility wordt hier ook mee afgedekt.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Waarde** | **Confidentiality** | **Integrity** | **Availability** | **Reliability** | **Accountability** | **Score** |
| Weging | 0.170703664 | 0.16551735 | 0.265678634 | 0.259769465 | 0.138330884 | - |
| Encryptie | 1 | 0 | 0.25 | 0 | 0.25 | 0.271706 |
| Autorisatie (wachtwoorden) | 0.75 | 0.5 | 0.25 | 0.25 | 1 | 0.480479 |
| RFID Authenticatie | 0.75 | 0.5 | 0.75 | 0.5 | 0.5 | 0.609096 |
| Monitoring | 0.25 | 1 | 0.75 | 1 | 1 | 0.805553 |

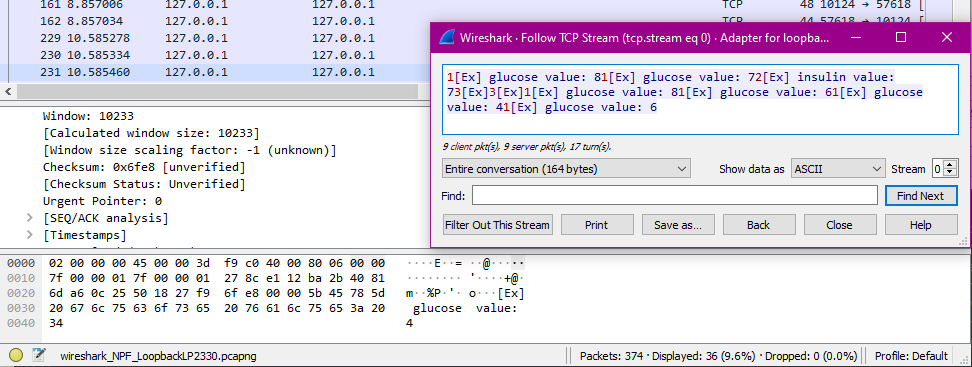
Na het bepalen van de verschillende weging van de criteria, zijn er waardes toegekend aan alle methodes en de bijbehorende criteria.

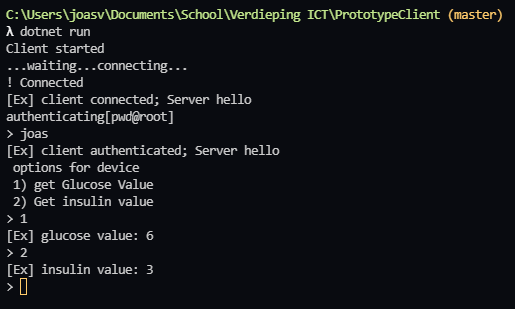
Hieruit kunnen we de volgende lijst opstellen:

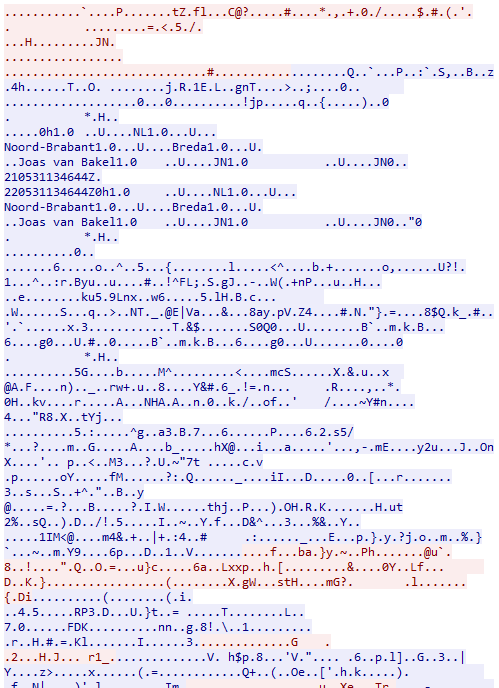
1. Monitoring (0.80)
2. RFID Authenticatie (0.61)
3. Autorisatie (0.48)
4. Encryptie (0.27)

Om de laatste deelvraag te beantwoorden is er voor gekozen om een prototype te bouwen. Om het prototype zo dicht tegen de werkelijkheid aan te zetten is er voor gekozen om een server op te zetten om vervolgens daar via een netwerkverbinding aan tegen te praten. Om te kijken of er verschil in de ontwikkeltijd zullen alle genoemde aspecten die eerder behandelt zijn in de MCA terug komen in de beveiligde versie van de applicatie.

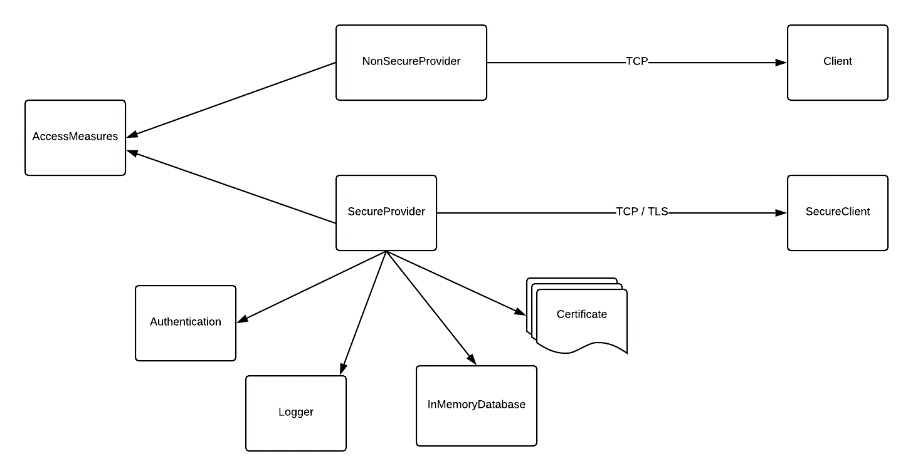
De ontwikkelperiode voor de onbeveiligde versie van de applicatie was ongeveer twee uur. Hier hadden we dan een simpele client server principe opgezet waarmee de glucose en insuline waardes konden worden gemeten. Zoals te zien is in het figuur hieronder is de communicatie gedaan via TCP, maar wel in normaal tekst formaat. Dit zou de applicatie dus kwetsbaar maken voor het onderscheppen van de verzonden informatie.



 De ontwikkelperiode voor de beveiligde variant van de applicatie duurde hierbij zeker langer. In zijn totaliteit ongeveer vier a vijf uur langer. Hierbij moesten namelijk meerdere aspecten geïmplementeerd worden. Een van deze elementen was de versleuteling van de berichten zodat deze niet meer zomaar gelezen konden worden. Hiervoor moest er een certificaat aangemaakt worden op de server zijde, aan de hand van het certificaat kon er vervolgens een TLS verbinding worden gemaakt. Hieronder de TCP-stream van de beveiligde applicatie:



Hierna moesten er natuurlijk andere klasses worden gerealiseerd die de autorisatie en monitoring regelde. Het monitoren van het apparaat gebeurde door middel van een logging klasse waarbij de verschillende handeling werden vastgesteld. De autorisatie van het apparaat werd afgehandeld door de Authentication klasse, deze klasse hashde de gegeven input en keek of deze overeen kwam met de InMemoryDatabase hash. Een klein high level diagram om het een en ander te verduidelijken:



De code voor het project is onder deze link te vinden:

<https://github.com/Joasv/verdieping-ict-app-prototype.git>

**Conclusie**

Om antwoord te geven op de vraag: “Hoe wordt beveiliging gerealiseerd bij monitoringsapparaten die glucosewaardes in het bloed meten” is er eigenlijk geen simpel definitief antwoord. Dit omdat de beveiliging van erg persoonlijke informatie altijd wel een kat en muis spel blijft. Waarbij de aanvallers en beveiligers van het geheel elkaar elke proberen te pakken. Wel is duidelijk dat er naar veel aspecten gekeken moet worden, mocht in de nabije toekomst een bedrijf beslissen dit soort apparaten te gaan produceren. Voorbeelden hiervan zijn bijvoorbeeld: garantie van integriteit, versleuteling van data en inperking van kwetsbaarheden. Daarbij moet er een goed keuze gemaakt worden in wat voor middelen er gebruikt gaan worden om die inperking van kwetsbaarheden te gaan realiseren. Hierbij is monitoring en encryptie een van de belangrijke middelen om dit te realiseren. Tot slot zien we ook dat goede beveiliging erg veel tijd neemt, ondanks de snelle innovaties op functioneel gebied. Echter blijft een goed beveiligd product leveren een lastig aspect, maar dit is ook te danken aan de morele aspecten die zich hier in mengen.

# Bibliografie

Ahmed A. Mawgoud, A. I. (sd). *Arxiv.* Opgehaald van A Secure Authentication Technique in Internet of Medical: https://arxiv.org/ftp/arxiv/papers/1912/1912.12143.pdf

Senrio. (2017, 6 5). *Medical Device Integrity*. Opgehaald van Senrio: https://blog.senr.io/blog/medical-device-integrity

Somayeh Nasiri, F. S. (2019, december 27). *Security Requirements of Internet of Things-Based Healthcare System: a Survey Study*. Opgehaald van NCBI PMC: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7004290/

1. Een whitelist (= een witte lijst) is eigenlijk een verzameling van entiteiten die als geautoriseerd (en vaak valide) worden beschouwd. [↑](#footnote-ref-1)