INTERNET OF THINGS I SUNDHEDSBRUG

En sikkerhedsanalyse

Internet of Things (IoT) opnår stigende udbredelse i samfundet, herunder sundhedssektoren. Desværre er informationssikkerheden i disse enheder ofte mangelfuld. Der undersøges, om datatrafikken i et sundheds-IoT-system er forsvarligt sikret. IoT-systemet, som undersøges, er udlånt af en virksomhed og er et system til lokationssporing af demente personer. Sikkerhedsundersøgelsen bliver lavet med udgangspunkt i begreberne confidentiality, integrity og availability. Til at undersøge sikkerheden samt underbygge de fundne sårbarheder udarbejdes en litteraturundersøgelse, hvor informationen søges frem i udbredte tidsskrifter. Desuden laves en forsøgsopstilling til undersøgelsen. Ud fra undersøgelserne kan det ses, at der primært er udfordringer med sikkerheden ift. kodeord samt med kommunikationsprotokoller. Undersøgelserne resulterer i en tjekliste, hvor sårbarheder er listet, samt henvisning til begreberne C, I og A (confidentiality, integrity og availability), og der gives anbefalinger til håndtering af sårbarhederne. Denne tjekliste er tiltænkt IT-ansvarlige i kommuner, på plejehjem mv., som kan bruge listen ved indkøb af sundheds-IoT-udstyr.

FORFATTERE
Henning Thomsen, ph.d., adjunkt, IT-uddannelserne, UCN
Simon Kongshøj, lektor, IT-uddannelserne, UCN
Ib Helmer Nielsen, lektor, IT-uddannelserne, UCN
Henrik Munk Hvarregaard, lektor, IT-uddannelserne, UCN
Per Trosborg, lektor, IT-uddannelserne, UCN

INDLEDNING

IoT er et begreb, som har fået stigende betydning i det moderne samfund. Dette gælder både inden for områder såsom smarte hjem, sundhed samt sporing af genstande såsom biler, cykler mv. IoT er kendetegnet ved, at de enheder, som indgår i et sådant system, ikke er direkte styret af mennesker, men fungerer autonomt.

IoT er efterhånden blevet særdeles udbredt, herunder til sundhedsbrug. Her kan nævnes enheder såsom fitnesstrackere, blodtryksmålere og intelligente personvægte. Disse er, som andre IoT-enheder, forbundet til internettet, og brugeren og/eller dennes hjælper kan så se status fra f.eks. fitnesstrackeren på sin smartphone. I artiklen ses kun på

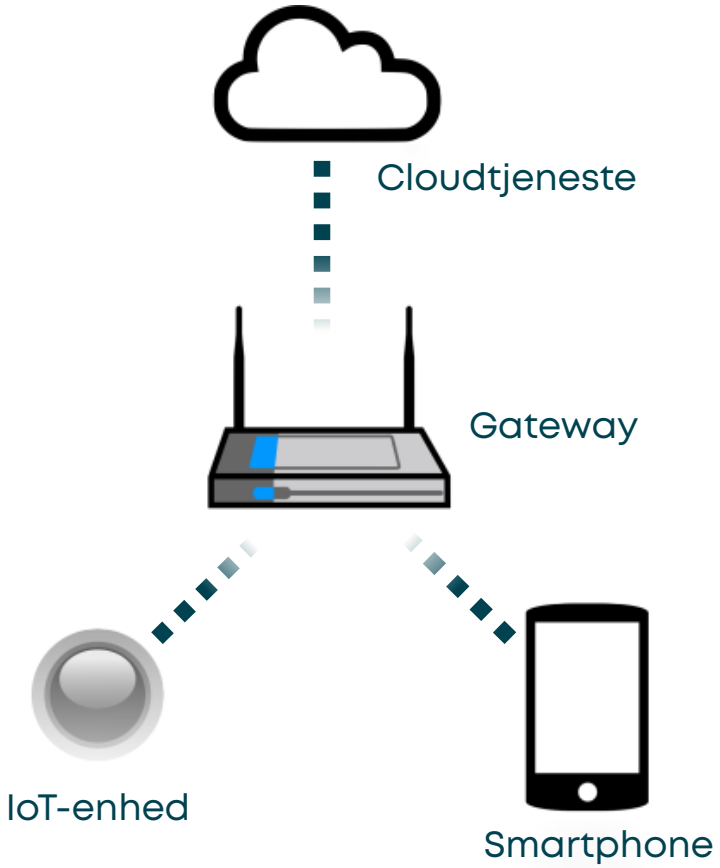
sundheds-IoT-enheder, som bliver anvendt i borgerens hjem og på plejehjem. IoT-enheder, som bliver anvendt på sygehuse, er ikke indbefattet i undersøgelserne.

Denne artikel er udarbejdet i forbindelse med et forskningsprojekt, "IT-sikkerhed inden for Sundheds-IoT", som er et samarbejde mellem IT-uddannelserne på UCN, forskningsprogrammet Teknologier i Borgernær Sundhed ved UCN samt en virksomhed, som fremstiller sporingsenheder til demente personer. I forskningsprojektet sigtes mod at udarbejde en tjekliste, som IT-ansvarlige personer ved kommuner, plejehjem mv. kan bruge, når de planlægger indkøb af IoT-udstyr til sundhedsbrug.

Arkitekturen i en generisk IoT-løsning er vist i figur 1. På figuren ses en IoT-enhed, som kommunikerer til og fra en central enhed, kaldet en gateway. Mange IoT-enheder til sundhedsbrug har en tilhørende app, som brugeren skal installere på sin smartphone. Denne app bruges f.eks. til at vise status for IoT-enheden og give brugeren et overblik over enheden – eller enhederne, såfremt der er flere. Brugerens smartphone (og evt. computer og/eller tablet) kan også kommunikere med IoT-enheden via gatewayen. Endelig er IoT-systemet typisk forbundet til en cloudtjeneste. Formålet med denne er bl.a. at lave databehandling, som så efterfølgende bliver vist for brugeren.

I de senere år er der sket en stor stigning i antallet af IoT-enheder, som er forbundet til internettet, og denne tendens viser en seksdobling i antal forbundne enheder fra 2012 til 2020 (Burhan, et al., 2018). Producenter af IoT-enheder er ofte meget interesserede i at få deres enhed først på markedet. Dette medfører ofte, at IT-sikkerheden i disse enheder ikke har førsteprioritet (O'Connor, et al., 2019). Endelig har det medført mange brud på IT-sikkerheden, hvor udefrakommende personer (såsom hackere) har kunnet se personfølsomt data fra sådanne IoT-enheder.

Figur 1: Kommunikationsveje i et IoT-system, (udarbejdet af forfatterne, 2021.)



Inden for sundheds-IoT er korrekt og ansvarlig håndtering af personfølsomme data særdeles vigtigt, men det er langtfra altid tilfældet, at sådanne data bliver beskyttet og håndteret forsvarligt. Dette har motiveret til at undersøge IT-sikkerheden i sundheds-IoT nærmere, hvilket er fokus i denne artikel. Denne artikel er struktureret på følgende måde:

I næste afsnit beskrives problemstillingen, som behandles, efterfulgt af baggrundsteori, som benyttes til at underbygge denne problemstilling og dennes løsning. Dernæst bliver metoden beskrevet, herunder forsøgsopstillingen. Dette efterfølges af en analyse af resultaterne. Dernæst konkluderes på artiklen, og der gives forslag til videre arbejde. Artiklens opbygning er vist på figur 2.

PROBLEMSTILLING OG MOTIVATION

Ud fra ovenstående er der nået frem til følgende problemstilling:

Hvilke sikkerhedsmæssige trusler og risici er der ved installation og ibrugtagning af IoT-enheder til sundhedsbrug, herunder sårbarheder inden for datakommunikation og -lagring.

KARAKTERISERING AF SUNDHEDS-IOT

Sundheds-IoT er en gren af IoT som er i kraftig vækst, og der forventes en firedobling i markedsværdien på

Figur 2: Oversigt over artiklens opbygning. (Figuren er udarbejdet af forfatterne, 2021.)

globalt plan fra 2018 – 2022 (Taylor, et al., 2018). Dette er formentligt en konsekvens af det øgede fokus på sundhed og velvære i samfundet, øgede krav om digitalisering – smartphonens udbredelse. Eksempler på anvendelser er fitnesstrackere, persontrackere, blodtryksmålere, intelligente personvægte, blodsukkermålere mv. Ligesom det er tilfældet i "almindelig" IoT, følger sundheds IoT også den samme overordnede opbygning (se figur 1), samt dataforbrug, strømforbrug mv. Der kan dog være forskelle, f.eks. bruger IoT-enheden, som vi undersøger i denne artikel ikke en gateway, men kommunikerer direkte til en cloudtjeneste. Kommunikationen i IoT-systemer er typisk autonom.

SIKKERHEDSMÅL

Inden for IT-sikkerhed anvendes CIA-triaden. Denne står for confidentiality, integrity og availability (Pfleeger, et al., 2015). På dansk er dette hhv. fortrolighed, integritet og tilgængelighed. Disse begreber er udbredt inden for sikkerhedsanalyse, specielt ifm. klassifikation af sårbarheder (Pfleeger, et al., 2015). I en IoT-kontekst betyder fortrolighed, at udefrakommende personer ikke kan læse de data, som bliver sendt mellem komponenterne i systemet (IoT-enheden, gateway og servere). Det betyder også, at data, som gemmes på komponenterne, bliver sikret. Integritet betyder, at uvedkommende ikke kan ændre i de data, som bliver sendt eller er gemt. Tilgængelighed betyder, at systemet (herunder data) skal være tilgængeligt for autoriserede brugere.

Fortrolighed, integritet og tilgængelighed er *sikkerhedsmål* for et IoT-system. Fortrolighed opnås eksempelvis vha. kryptering af datatrafikken. Integritet opnås eksempelvis igennem autentificering af datatrafikken, og endelig kan tilgængelighed opnås ved at blokere for uvedkommende trafik udefra. I yderste konsekvens kan ændringer i data have alvorlige konsekvenser for patient, behandlere og pårørende.

Brud på fortrolighed sker ofte, når datatrafikken ikke er tilstrækkeligt beskyttet mod læsning af udefrakommende. Dette sker ofte ved, at datatrafikken ikke er krypteret (eller at krypteringen ikke har tilstrækkelig kvalitet). Brud på integritet sker, når der ikke er tilstrækkelig validering af datatrafikken. Dette sker ofte, hvis de metoder, som bliver brugt til validering, er forældede eller uegnede til formålet. Endelig sker brud på tilgængeligheden når IoT-enheder (her tænkes specielt på cloudtjenesten) bliver udsat for en stor mængde forespørgsler inden for kort tid. Dette medfører, at de bliver utilgængelige.

METODE

I projektet bruges design and development research (Ellis & Levy, 2010), hvilket er en udbredt fremgangsmåde inden for forskning i emner vedrørende IT, herunder IT-sikkerhed. Dette er kendetegnet ved, at forskningen resulterer i et artefakt, som kan anvendes af målgruppen. I nærværende tilfælde er artefaktet en tjekliste, og målgruppen er IT-ansvarlige i kommuner og regioner.

Design and development research er kendetegnet ved, at der er seks trin i forskningen. Første trin er identificering af problemet, efterfulgt af en beskrivelse af målene. Dernæst skal et artefakt designes og udvikles. Dette kan være et softwareprodukt, en anbefaling eller lignende. Fjerde trin er test af artefaktet, og trin fem er evaluering af testen. Det sidste trin er formidling af resultaterne.

I første trin er litteraturen omhandlende IT-sikkerhed undersøgt mhp. at få et overblik over, hvilke sårbarheder der er relevante og udbredte inden for IoT. I trin to er målene i projektet beskrevet i form af en problemformulering. Det tredje trin er design af et artefakt, som i denne artikel er en tjekliste. I det fjerde trin tages udgangspunkt i en case, hvor sikkerheden bliver testet. Evalueringen af testen, som er det femte trin, munder ud i tjeklisten. Det sidste trin er formidling i form af nærværende artikel. Se figur 2 for artiklens opbygning.

RELEVANT LITTERATUR

I litteraturstudiet undersøges artikler udgivet på konferencer såsom USENIX Security Symposium, IEEE Security & Privacy Conference og ACM SIGCOMM samt mere uformelle publikationskanaler såsom hjemmesider, blogs mv. af ledende forskere inden for IT-sikkerhed.

Artiklen (Newaz, et al., 2020) er en oversigtsartikel over 96 artikler vedrørende IT-sikkerhed, som behandler og kategoriserer angrebstyper inden for IoT til sundhedsbrug. De når frem til, at 24 % af angrebene påvirker fortrolighed, 44 % påvirker integritet, og 32 % påvirker tilgængelighed. De viser også, at 37 % af angrebene er på invasive enheder (såsom pacemakere), 22,2 % af angrebene er på aktive terapeutiske enheder (såsom høreapparater) og 40,7 % er på ikke-invasive enheder.

I (Wood, et al., 2017) undersøger de omfanget og typen af informationslækage i forskellige IoT-enheder. Disse er blodtryksmålere, smarte personvægte og blodsukkermålere. I deres forskning laver de også et program, IoT-Inspector, som brugeren kan benytte til at se, hvor i IoT-systemet der er informationslækage, hvilket ofte skyldes manglende og/eller utilstrækkelig kryptering af data. De når frem til, at en del af de undersøgte enheder sender personfølsomme data (f.eks. blodtryk) ukrypteret, hvilket medfører, at uvedkommende kan læse disse data.

Manglende og utilstrækkelig kryptering bliver også undersøgt i (Loi, et al., 2017), hvori forfatterne undersøger 20 IoT-enheder for omfanget af kryptering sendt over tre kanaler: IoT-enhed til smartphone, smartphone til cloud og

IoT-enhed til smartphone. De når frem til, at de fleste tilfælde af manglende kryptering sker i kommunikationen mellem IoT-enhed og smartphone, mens de andre to kanaler er sikret ret godt. Desuden bliver der vist, at mange enheder lagrer vigtige data (personoplysninger og -målinger) ukrypteret.

En sikkerhedsundersøgelse af en fitnesstracker, som bruger Bluetooth er udført i (Mendoza, et al., 2018). Heri undersøges en fitnesstracker samt dennes tilhørende app og cloudløsning. Deres hovedkonklusion er, at appen bruger http Basic Authentication ifm. brugergodkendelse. Dermed sendes e-mail og kodeord ukrypteret til serveren, hvilket gør, at det er muligt at aflytte disse.

Ud fra ovenstående ses, at der er store udfordringer med fortrolighed i form af manglende og svag kryptering. Disse mangler findes i alle kommunikationskanaler i IoT-systemer. Desuden ses, at der er svagheder med autentificering, blandt andet ift. kodeord. En anden mangel er opdatering og registrering af enheder. Det ses, at sårbarhederne er inden for alle tre grene af CIA.

TJEKLISTER OG ANBEFALINGER

Indenfor IoT har flere aktører udarbejdet oversigter, top-10-lister over sårbarheder og tjeklister til IoT enheder, programmer og opsætning. En udbredt top-10-liste er OWASP IoT Top-10 (OWASP, 2017). Denne liste er resultatet af input fra udviklere, hvor de identificerer de 10 alvorligste sårbarheder inden for IoT. Sårbarhederne på denne liste relaterer sig både til selve IoT-enheden, dennes gateway, cloudløsning samt web- og appløsning. På listen er sårbarhederne delt i tre dele, netværkssikkerhed, softwaresikkerhed (programsikkerhed) og fysisk sikkerhed. Netværkssikkerhed henviser til kommunikationen imellem de enkelte dele i løsningen (se figur 1), herunder manglende/svag kryptering, utilstrækkelig autentificering (af enheder og brugere) samt netværkstjenester, som accepterer indgående forbindelser unødvendigt.

Et element, som er højt på denne liste, er valg af kodeord. Dette er et punkt, som ikke udelukkende er et problem ved IoT, men også inden for andre IT-områder. Konkret er der tale om, at kodeordene er for korte, eller at de allerede findes i en ordbog. Dette gør det nemt for udefrakommende personer at lave automatiserede programmer, som tester alle mulige kodeord mhp. at få adgang til IoT-systemet (og dermed brugerens data). Ansvarligt valg af kodeord beror på, at uvedkommende personer ikke kan gætte sig frem til kodeordet. Et godt udgangspunkt i denne sammenhæng er, at kodeordet er mindst 10 tegn og indeholder små og store bogstaver, tal samt specialtegn. Desuden bør kodeord ikke kunne findes i en ordbog (Zhang-Kennedy, et al., 2016).

Opdatering af IoT-enheder er også et sårbarhedspunkt. Selve IoT-enhederne kører noget firmware. Denne firmware skal ligesom alle andre programmer sikkerhedsopdateres, når der er behov for det. En udfordring heri, som også er blevet påpeget i (Ly & Jin, 2016) ifm. undersøgelse af fitnesstrackere, er, at denne firmware ikke er valideret af fabrikanten. Dette medfører, at det i teorien er muligt for udefrakommende personer at installere en modificeret firmware på en sådan enhed. Inden for CIA er dette et brud på integritet.

En anden liste er IoT-tjekliste til virksomheder, udarbejdet af Rådet for Digital Sikkerhed (Rådet for Digital Sikkerhed, 2020). I lighed med OWASP-listen har denne fokus på adgangskoder. Desuden er der også fokus på netværkssikkerhed såsom opdeling af netværk (så IoT-enhederne er på et separat netværk), frakobling af UPnP (UPnP står for Universal Plug and Play og gør det muligt for IoT-enheden at åbne for adgang til udefrakommende trafik uden brugerens eksplicitte samtykke) og kryptering af datatrafik og -lagring.

SUNDHEDS-IOT-ENHEDEN, SOM BLIVER UNDERSØGT

Til at undersøge IT-sikkerheden i et konkret produkt er et IoT-produkt udlånt til personsporing af en samarbejdspartner. Dette produkt er tiltænkt ældreplejen og bruges både af personer med mild demens (som p.t. bor hjemme) samt personer med svær demens, som bor på et plejehjem. De enkelte komponenter i produktet er vist på figur 3.

Figur 3: De enkelte komponenter i IoT-enheden, som undersøges.

Billedet er udarbejdet af forfatterne, 2021

Selve produktet, som vist på figuren, består af en brik (polet), som den demente person skal have i lommen. Desuden består systemet af en base, som skal placeres i borgerens hjem eller plejehjem. Denne base indikerer for systemet, hvor borgerens hjem er. Når brikken ikke er inden for basens rækkevidde, vil dette opfattes som, at borgeren ikke er i sit hjemmeområde. Systemet består også af en app, som plejepersonalet installerer på deres smartphone. Denne app viser status for de personer, som har bevæget sig uden for deres hjemmeområde (enten hjemme hos sig selv eller på plejehjemmet). Systemet består også af en oplader til trådløs opladning af brikken.

Ud fra vores litteratursøgning, søgning i eksisterende tjeklister samt med udgangspunkt i den udlånte enhed behandles følgende spørgsmål:

(1): Er der nogen regler for valg af kodeord, i så fald hvilke?

(2): Er datakommunikationen og -lagringen i IoT-systemet sikret tilstrækkeligt, og er det muligt at måle dette (også automatisk)?

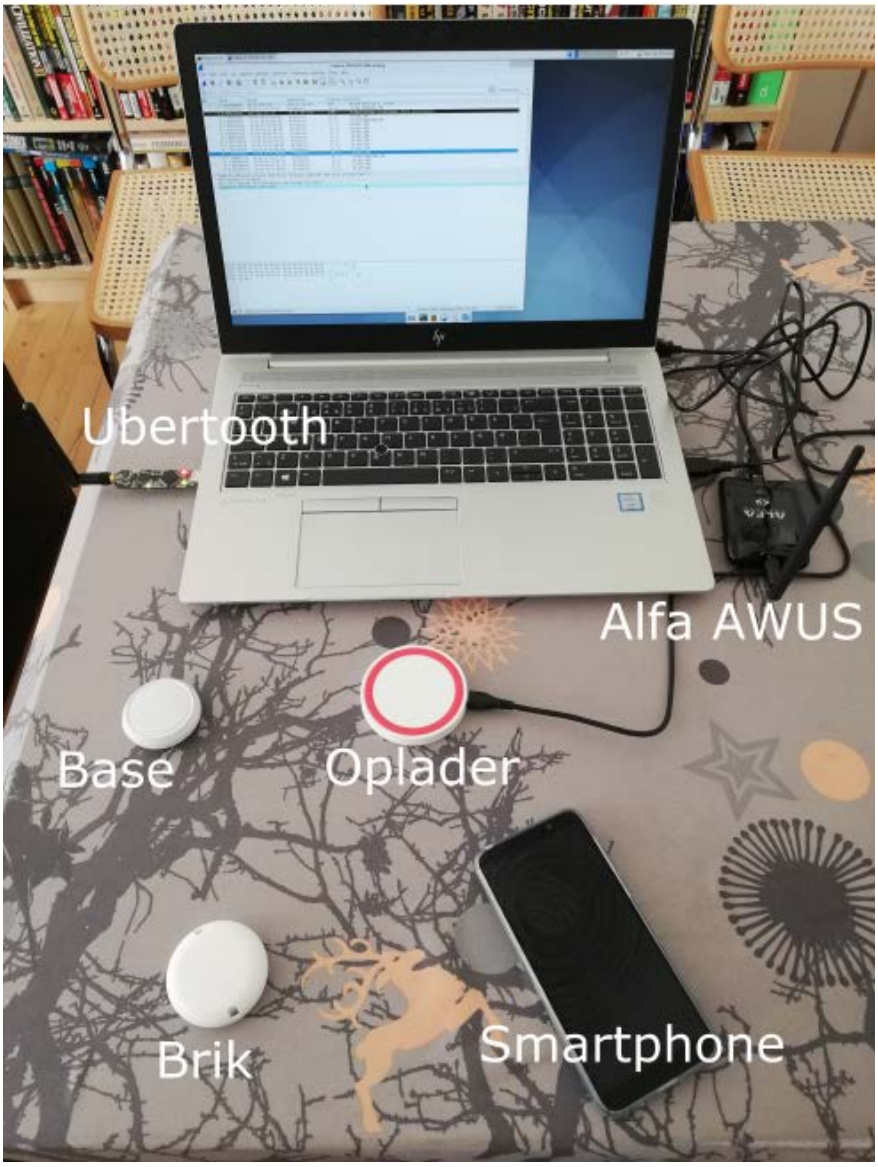
(3): Er det muligt at forfalske basen i IoT-systemet og dermed sætte systemet i en tilstand, hvor det altid er i alarm?

(4): Er det muligt at aflytte og/eller ændre datatrafikken mellem IoT-enheden (både brik og base) og dennes app?

FORSØGSOPSTILLING

Vores forsøgsopstilling er vist på figur 4. Spørgsmålene 1, 2, 3 og 4 i forrige afsnit vil blive undersøgt med udgangspunkt i denne opstilling. På figuren ses brikken, som er den enhed, brugeren (f.eks. den demente person) skal have med sig. Desuden vises hjemmebasen. Der ses også en smartphone, hvorpå den tilhørende app bliver installeret. Endelig vises en laptop til dataopsamling og -behandling, inklusiv udstyr til at undersøge Bluetooth Low Energy- (BLE) trafik (Ubertooth

Figur 4: Forsøgsopstillingen.



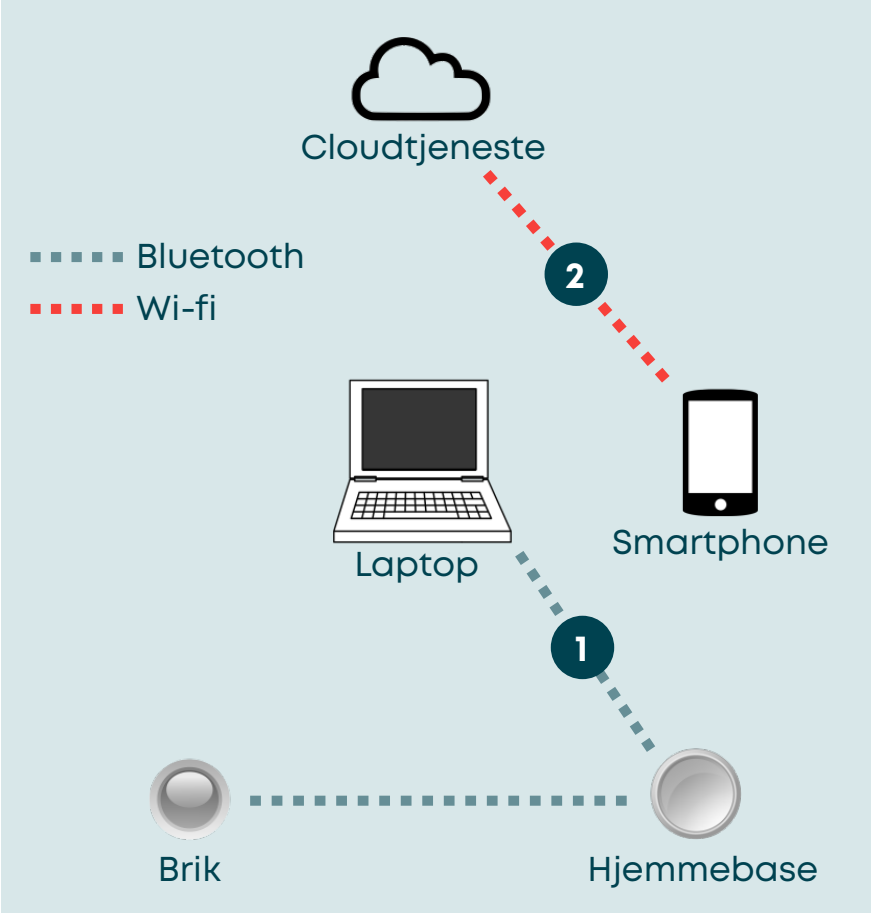
Billedet er udarbejdet af forfatterne, 2021

på figuren) samt wi-fi-trafik (Alfa AWUS på figuren). Dette er i overensstemmelse med en typisk IoT-opstilling (se figur 1).

Brikken sender regelmæssige lokationsdata via Narrow-Band IoT (NB-IoT) til cloudserveren. NB-IoT er et landsdækkende telenetværk tiltænkt IoT-enheder. Hjemmebasen, som skal monteres i brugerens eget hjem eller plejehjem, sender regelmæssigt signaler (kaldet beacons) over BLE. Hvis brikken kan modtage disse BLE signaler, er den inden for rækkevidde og sender dermed ikke lokationsdata over NB-IoT. Hvis den modsat ikke kan modtage disse signaler, opfattes det som, at brikken (og dermed personen, som bærer den) er uden for sit hjem/plejehjem, og dermed sendes en alarm til cloudserveren samt en alarm til smartphonen. Appen kommunikerer med en cloudserver. På figur 5 er vist et diagram over enheden og kommunikationsveje, herunder de målepunkter, som er relevante for vores undersøgelser.

I forsøget måles BLE-trafik (indikeret med et "1" på figuren) og wi-fi-trafik (indikeret med et "2"). Førstnævnte bliver målt med en Ubertooth One r161-p14, som er en enhed, der kan opsamle BLE-trafik. Wi-fi-trafik bliver målt med en Alfa

Figur 5: Kommunikationsveje og -målepunkter i opstillingen.
(Figuren er udarbejdet af forfatterne, 2021.)



AWUS036NHA wi-fi-usb-dongle. Begge enheder tilkobles en HP EliteBook 850 G6 laptop, og selve datatrafikken (BLE og wi-fi) opsamles og undersøges med programmet på denne laptop.

Ud over ovenstående undersøgelser er der lavet en brugstest af enheden. Der er fra fabrikantens side oprettet en brugerkonto til formålet. Følgende er undersøgt:

1. Er kodeordet ved oprettelse af bruger fra fabrikantens side sikkert og forsvarligt?
2. Ved skift af brugerens kodeord: Hvilke regler er der ved valg af nyt kodeord (længde af kodeord, valg af tegn i kodeordet, genbrug af gammelt kodeord)?

RESULTATER

I dette afsnit besvares spørgsmålene 1, 2, 3, og 4, som er fundet ved undersøgelsen i forrige afsnit.

Det første spørgsmål vedrører valg af kodeord. Der er, ud fra undersøgelserne, ikke noget krav om at ændre kodeordet ved sin brugerprofil, efter at denne er oprettet fra fabrikantens side. Ved valg af nyt kodeord viser testen, at korte kodeord (mindre end 10 tegn) samt kodeord, som kan findes i en ordbog, accepteres. Desuden kan man, efter at have skiftet til et nyt kodeord, skifte tilbage til sit gamle kodeord igen. Dette er mangelfuldt jf. (Zhang-Kennedy, et al., 2016).

For at besvare spørgsmål 2 er datakommunikationen undersøgt (via wi-fi og Bluetooth), som vist i forrige afsnit. Vedrørende wi-fi (målepunkt 1 i figur 5) så benytter enheden sig af WPA-PSK2, hvilket i skrivende stund giver god beskyttelse både ifm. fortrolighed og integritet (Pfleeger, et al., 2015).

Selve datakommunikationen mellem smartphone og cloud er beskyttet med Transport Layer Security (TLS), hvilket giver god sikkerhed ift. fortrolighed og integritet. TLS er en udbredt standard til sikker datakommunikation på computernetværk.

Undersøgelsen af Bluetooth har vist, at produktet bruger en udfaset version af Eddystone-protokollen, hvilket kan udgøre en sikkerhedsrisiko.

Vedrørende spørgsmål 3, så er basen, som bliver brugt, et standardprodukt, og undersøgelserne har vist, at der er en mulighed for at forfalske denne base. Dette kan gøres ved at oprette en Bluetooth-enhed med samme MAC-adresse (en slags ID) som den eksisterende base. Selve brikken bruger enten Bluetooth eller NB-IoT, alt efter om den er inden for basens rækkevidde. Konsekvensen af en sådan forfalskning vil være, at brikken bliver opfattet som værende inden for rækkevidden, hvilket vil svare til, at brugeren vil blive opfattet som værende i sit hjem, selvom brugeren har bevæget sig uden for hjemmet.

Til at besvare spørgsmål 4 viser undersøgelserne, at det ikke er muligt at ændre datatrafikken pga. de anvendte stærke krypteringsmetoder. Det er heller ikke muligt at aflytte private data pga. samme årsag. Det er dog muligt at aflytte metadata. Heri kan være information om afsender og modtager i form af IP-adresser og/eller MAC-adresser.

Tabel 1 viser, ud fra litteratursøgningen og undersøgelserne af IoT-enheden, hvilke opmærksomhedspunkter der er relevante. Denne tabel viser også, hvilke af de tre sikkerhedsmål (CIA) der bliver kompromitteret. Desuden beskrives en anbefaling ud for hvert sårbarhedspunkt. Bemærk, at denne liste ikke er udtømmende, men primært baseres på svarene til spørgsmålene 1, 2, 3 og 4. Denne tabel kan anvendes som en tjekliste for IT-ansvarlige.

Tabel 1: Sårbarheder og anbefalinger ift. sikkerhedsanalysen, 2021. (Tabellen er udarbejdet af forfatterne).

Sårbarhed	Beskrivelse	Sikkerhedsmål kompromitteret	Anbefaling
Svage adgangskoder	Brugere bruger adgangskoder, som er for korte, med ord, som findes i en ordbog mv.	C, I	Kodeord bør være mindst 10 tegn, en blanding af små og store bogstaver, tal og specialsymboler.
Svag opdateringsmekanisme	Opdatering af firmware sker igennem ukrypterede datakanaler, selve firmwaren er ikke integritetstjekket.	I, A	Opdatering bør foregå igennem sikrede netværk og hentes fra pålidelig kilde. Opdatering af IoT-enhed bør ikke sendes via smartphone, men sendes direkte.
Standardkodeord på enheder	Enheder har standardkodeord fra fabrikantens side, f.eks. admin, root eller lignende.	C	Ved ibrugtagning bør disse udskiftes til forsvarlige kodeord.
Registrering af enheder	Enheder bliver koblet til IoT-systemet på en uforsvarlig/ad hoc-metode.	A	Administrator bør lave en liste over enhederne.
Aktivér kryptering af datatrafik	Ukrypteret datatrafik mellem IoT-enheden og internettet gør, at andre personer kan aflytte trafikken.	C, I	Der bør sikres, at enheder anvender tilstrækkelig kryptering: Bluetooth: som minimum version 5. Wi-fi: Brug WPA2-PSK eller WPA2 Enterprise.
Aflytning af datatrafik	En ordartet person kan aflytte datatrafikken, dog kun metadata.	C, I	Der bør sikres, at enheden kører på et separat netværk, som uvedkommende ikke har adgang til (netværkssegregering).

KONKLUSION

Ud fra litteraturstudiet samt casestudiet kan det udledes, at der er problemer med kryptering og autentificering af enhederne. Her skal specielt den manglende kryptering fremhæves. I litteraturen samt casestudiet er der observeret, at sikkert valg af kodeord ikke bliver håndhævet. Det kan her anbefales, at brugeren informeres om regler ifm. valg af kodeord. Casestudiet viser, at det er vigtigt at sikre brugerens data ved at anvende de nyeste krypteringsmetoder af højeste standard.

Der er givet et bud på en liste over sårbarheder samt anbefalinger ift. et IoT-system til sundhedsbrug. Denne liste er baseret på forskningsspørgsmålene, det dertilhørende litteraturstudie og undersøgelsen af IoT-enheden i casestudiet.

PERSPEKTIVERING

Resultaterne i denne artikel har en direkte anvendelse på uddannelser inden for teknologi og sundhed. På IT-uddannelserne er casen blevet brugt på professionsbachelor i IT-sikkerhed, i forbindelse med undervisning i faget IoT & Cloud. Den er blevet brugt som et eksempel på at vise de studerende, hvordan et IoT-system er opbygget, samt hvilke sikkerhedsaspekter der er relevante. Ligeledes tænkes resultaterne anvendt på IT-teknolog-uddannelsen, i forbindelse med faget Internet of Things.

Inden for sundhedsuddannelserne kan resultaterne f.eks. bruges i faget teknologi på sygeplejerskeuddannelsen mhp. at give de studerende mulighed for at se et eksempel på sundheds-IoT og på, hvad man skal være opmærksom på ift. IT-sikkerhed. Her tænkes f.eks. på anbefalingerne ift. kodeord på appen.

Undersøgelsen er afgrænset til at undersøge enheder inden for borgerens hjem og plejehjem. Fremtidige studier bør indeholde flere enheder inden for sundheds IoT for at få et mere fuldstændigt billede af sikkerheden. Desuden bør IoT-enheder anvendt på hospitalerne undersøges nærmere ift. sikkerheden, da disse har skærpede sikkerhedskrav. Her tænkes f.eks. på enheder såsom pacemakere.

Litteraturliste

- Burhan, M., Rehman, R. A., Kim, B.-S. & Khan, B., 2018. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors 18(9), 24 august, pp. 1-38.
- Ellis, T. J. & Levy, Y., 2010. A Guide for Novice Researchers: Design and *Proceedings of Informing Science & IT Education Conference (InSITE),* pp. 107-118.
- Jingjing Ren, D. J. D. D. C., Mandalari, A. M., Kolcun, R. & Haddadi, H., 2019. Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach. *Proceedings of the Internet Measurement Conference,* pp. 267-279.
- Loi, F. et al., 2017. Systematically evaluating security and privacy for consumer iot devices. *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy,* pp. 1-6.
- Ly, K. & Jin, Y., 2016. Security Studies on Wearable Fitness Trackers. *IEEE 38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society.*
- Mendoza, F. A. et al., 2018. Assessment of fitness tracker security: A case of study. *Multidisciplinary Digital Publishing Institute Proceedings,* pp. 12 - 35.
- Newaz, A. I., Sikder, A. K., Rahman, M. A. & Uluagac, A. S., 2020. A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defenses. *ArXiv preprint,* 15 maj, pp. 1-40.
- O'Connor, T., Enck, W. & Reaves, B., 2019. Blinded and confused: uncovering systemic flaws in device telemetry for smart-home internet of things. *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks,* Issue 140-150.
- OWASP, 2017. *Owasp top 10 - 2017: The ten most critical web application security risks.* [Online]
- Available at: https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf
- [Senest hentet eller vist den 19 februar 2021].
- Pfleeger, C. P., Pfleeger, S. L. & Margulies, J., 2015. *Security in Computing.* 5. red. s.l.:Pearson.
- Rådet for Digital Sikkerhed, 2020. *IoT-tjekliste til virksomheder.* [Online]
- Available at: https://sikkerdigital.dk/media/12542/iot-tjekliste-til-virksomheder.pdf
- [Senest hentet eller vist den 19 februar 2021].
- Taylor, K., Steedman, M., Sanghera, A. & Thaxter, M., 2018. *Medtech and the Internetof Medical Things: How connected medical devices are transforming health care,* s.l.: Deloitte.
- Wood, D., Apthorpe, N. & Feamster, N., 2017. Cleartext data transmissions in consumer iot medical devices. Proceedings of the 2017 *Workshop on Internet of Things Security and Privacy,* pp. 7-12.
- Zhang-Kennedy, L., Chiasson, S. & Oorschot, P. v., 2016. Revisiting password rules: facilitating human management of passwords. *IEEE 2016 APWG symposium on electronic crime research (eCrime),* pp. 1 - 10.