Utfordringer og fordeler ved bruk av biometriske autentikatorer for brukerautentisering

Mathias Greve Johannessen

Innhold

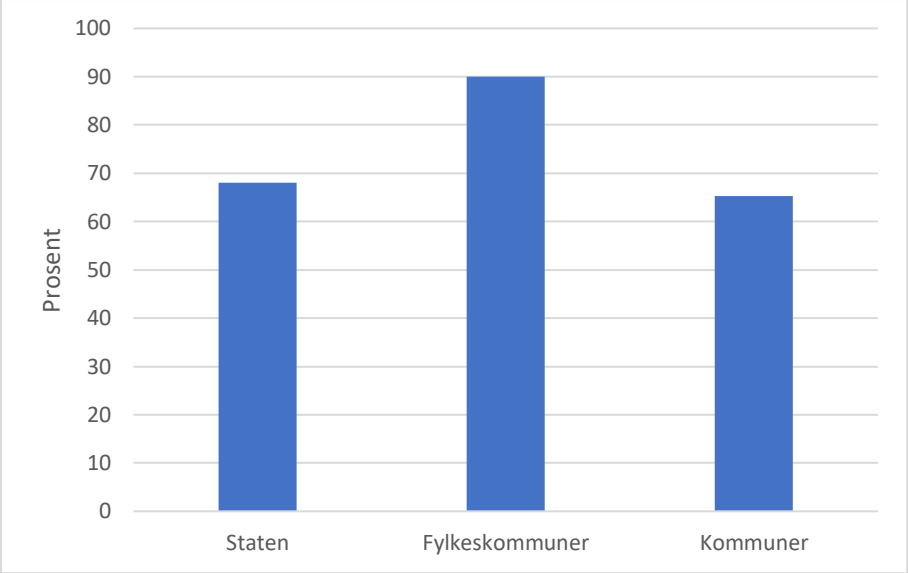
1 Innledning

Sikker brukerautentisering blir stadig viktigere i dagens samfunn der stadig større deler av våre liv baserer seg på digitale løsninger hvor brukerne må logge seg inn med sin digitale identitet. Flere land går blant annet i større grad over til e-forvaltning, der offentlige tjenester blir digitale (Jøsang, 2021). I tillegg viser undersøkelser gjort av Statistisk sentralbyrå (2021) at flere virksomheter i offentlig sektor benytter seg av digitale løsninger som baserer seg på innlogging med en digital identitet. Særlig har koronapandemien drevet denne utviklingen da flere ser mulighetene av å jobbe hjemmefra. For å autentisere seg, og bevise sin digitale identitet, til disse tjenestene som tar over flere og flere deler av livene våre, benyttes ulike metoder. Blant disse er konvensjonelle passord, enhets-baserte koder, og fysiologiske karakteristikker ved et individ benyttet som indikatorer for en digital identitet.

Tall fra en undersøkelse av digitalisering og IKT i offentlig sektor gjort av statistisk sentralbyrå i år, viser at forsøk på identitetstyveri er den mest forekommende sikkerhetstrusselen i 2022 (se Figur 1) (Statistisk sentralbyrå, 2022). Samtidig viser tall fra undersøkelse gjort av NorSIS og Skatteetaten at 3,4% oppga at de hadde blitt utsatt for identitetstyveri i løpet av de siste to årene (Skatteetaten, 2022). Det tilsvarer omtrent 150 000 nordmenn. En rapport fra ForgeRock (2022) hevder at antall forekomster av brukernavn- eller passord-lekkasje var på over 2 milliarder i 2021 og at dette var en økning på 35%.

Figur 1

Forsøk på identitetstyveri (phishing) i offentlig sektor



Notat. Svar fra årets undersøkelse av virksomheter i offentlig sektor som viser forsøk på identitetstyveri (phishing) i løpet av de siste tolv månedene angitt i prosent.

På bakgrunn av slike tall som nevnes i paragrafen over har FIDO Alliance uttalt at autentisering som utelukkende belager seg på passord er et av de største sikkerhetsproblemene på nettet (Glavin, 2022). Med støtte fra store internasjonale virksomheter som Apple, Microsoft og Google har FIDO Alliance sammen med World Wide Web Consortium utarbeidet en passord-fri innloggings-standard. Denne standarden baserer seg på blant annet biometrisk autentisering og offentlig/privat-nøkkel

kryptografi. Det er ventet at de nevnte virksomhetene i tillegg til flere andre virksomheter vil begynne å benytte seg av denne passord-frie innloggingsstandarden i løpet av 2023.

Mulighetene for bruk av biometrisk autentisering for å verifisere oss til disse digitale tjenestene øker også i større grad nå som flere av oss har mobiltelefoner og andre bærbare enheter med oss til enhver tid. Disse enhetene er i større grad utstyrt med integrert hardware med sensorer som kan måle biometriske autentikatorer.

Grunnet den økende tilgjengeligheten og forekomsten av biometriske løsninger vil denne artikkelen ta for seg hva biometrisk autentisering er i tillegg til å diskutere fordeler og ulemper ved biometrisk brukerautentisering. Det er kritisk at bruk av de digitale tjenestene vi er omgitt av overalt i dag gjøres så sikkert som mulig for å forhindre skader på informasjon og trusler mot personvern, men er også viktig for å sikre at korrekte individer får tilgang hos større forretninger for å sikre sikkerhetsmålene hos organisasjoner/bedrifter.

Med det som belyses i denne artikkelen, håper jeg å kunne bidra til en mer velinformert og sikker anvendelse av biometriske løsninger for brukerautentisering i fremtiden, og at både brukere og virksomheter blir kjent med dets fordeler og utfordringer.

2 Autentisering

For å kunne ha en fornuftig diskusjon om fordeler og utfordringer ved biometrisk autentisering er det nødvendig å etablere noe forkunnskap om konseptet autentisering og hvordan biometriske målinger implementeres. Oppgaven vil derfor begynne med å definere hva autentisering er og dets rolle i informasjonssikkerhet, i tillegg til å gi et oversiktsbilde av hva biometrisk autentisering er og hvordan et system for biometrisk autentisering kan se ut.

Autentisering defineres som «en handling, prosess, eller metode som viser at noe (som for eksempel en identitet) er ekte, sant eller genuint» (Merriam-Webster, n.d.). For temaet i denne oppgaven vil begrepet i hovedsak omhandle å bevise at en menneskelig bruker av en digital tjeneste faktisk er den denne personen utgir seg for å være. Det finnes ulike former for autentisering som kan organiseres hierarkisk, med *entitets-autentisering* og *data-autentisering* som de to overordnede typene. Under paraplyen til entitetsautentisering inkluderes *brukerautentisering* og *systemautentisering*.

Entiteten her er en menneskelig aktør, et individ, som autentiseres ved å bevise sin identitet til systemet den forsøker å autentisere seg til. For å bevise sin identitet til systemet benyttes *autentikatorer*. Autentikatorer kan være blant annet passord, koder man mottar på brikker eller andre enheter, eller fysiologiske attributter ved individet. Ulike autentiseringsmetoder benytter ulike autentikatorer. Ved å bevise at brukeren faktisk er den den utgir seg for å være, bidrar dette til å sikre at riktige individer får tilgang slik de er autorisert til i henhold til den gitte tilgangspolicyen. Dette fører til at data og tjenester kun gjøres tilgjengelig for bruk og interaksjon for de med riktig autorisasjon. Korrekt autentisering gir dermed støtte for sikkerhetsmålene om konfidensialitet og integritet.

Det er vanlig å dele autentiseringsmetoder i tre ulike kategorier eller faktorer – noe man *vet*, noe man *har* og noe man *er*. Disse tre faktorene er altså enten kunnskapsbaserte, eierskapsbaserte eller er iboende egenskaper ved entiteten. Autentikatorer for den første kategorien inkluderer konvensjonelle passord eller PIN-koder. I den andre kategorien er autentikatoren gjerne en kode man får tilsendt til en enhet man besitter, for eksempel en brikke eller mobiltelefon. Den siste

kategorien omfatter iboende egenskaper ved individet – unike, fysiologiske attributter. Ofte inkluderes det i denne kategorien også noe man gjør i form av atferds-attributter, for eksempel hvordan en beveger eller oppfører seg. Det er i denne siste kategorien, eller faktoren, vi finner biometrisk autentisering, som vi skal se nærmere på i neste seksjon av oppgaven.

3 Biometrisk brukerautentisering

Det finnes to ulike tilnærminger for hvordan biometrisk autentisering benyttes. En metode fungerer som «en-til-en»-undersøkelse, omtalt som *verifisering*, mens den andre er «en-til-mange», kalt *identifisering*. Disse har ulike bruksområder. Hvilke metode man bruker avhenger av hvorvidt man vet identiteten til personen, eller ikke, og hvorvidt den biometriske gjenkjenningen skal benyttes til å identifisere en ukjent person eller verifisere en kjent identitet. Identifisering benyttes blant annet i overvåkning, der man på bakgrunn av biometrisk informasjon fra mange individer ønsker å identifisere én person blant disse mange forskjellige. I verifisering, derimot, får man en oppgitt identitet og som man deretter benytter biometriske metoder for å verifisere at personen faktisk tilhører den identiteten den har oppgitt. Grunnet oppgavens tema om brukerautentisering, vil det videre fokuseres på verifiseringstilnærmingen.

Et begrep som benyttes i litteraturen når man snakker om biometrisk verifisering er *gjenkjenning*. Biometrisk gjenkjenning er et begrep som benyttes om verifisering av entiteter, og defineres av «International Organization for Standardization» (ISO) (2018) som «automatisert gjenkjenning av individer basert på deres biologiske- eller atferdskarakteristikker». Prosessen går ut på å kjenne igjen mønstre i menneskelig atferd eller fysiologiske trekk, og på bakgrunn av dette verifisere identiteten til individet som undersøkes.

I biometrisk brukerautentisering brukes fysiologiske egenskaper ved et individ til å verifisere identiteten til individet. Den biometriske autentikatoren er en målbar fysiologisk egenskap ved individet, som for eksempel fingeravtrykk, iris eller ansiktsmønster. Disse ulike fysiologiske egenskapene kalles også modaliteter, og jeg kommer til å bruke ordet «modalitet» eller tilsvarende «biometrisk modalitet» videre i oppgaven. For å omtale de grunnleggende elementene som modalitetene består av, og som gjør de unike, vil jeg benytte ordet «karakteristikk». For eksempel er et fingeravtrykk en modalitet, mens de unike mønstrene i fingeravtrykket er karakteristikkene.

Det stilles noen generelle krav for hva en modalitet må ha av egenskaper for å kunne anvendes. Disse er *universalitet*, *særpeg*, *permanens* og *målbarhet* (Jain et al., 2004; Jøsang, 2021). For at en modalitet skal kunne benyttes som autentikator er det først og fremt nødvendig at den kan detekteres av en sensor og representeres kvantitativt. Det må være mulig å ta bilde av og finne karakteristikker som utgjør et mønster som kan representeres med tall. Det er også viktig at den er universell, i form av at så mange som mulig har denne modaliteten. Det ville vært lite hensiktsmessig å benytte en modalitet som kun en liten del av befolkningen har, og dermed kunne bare denne lille andelen mennesker kunne autentisere seg. I tillegg til universalitet og målbarhet inkluderes også særpreg og permanens for hva en modalitet er nødt til å ha av egenskaper. Modaliteten må altså henholdsvis være tilstrekkelig ulik fra person til person slik at man kan identifisere unike personer og den må være relativt uendret over tid.

For å eksemplifisere de universelle kravene, ville håret man har på hodet vært en relativt dårlig modalitet for biometrisk autentisering. Det er mulig å måle og representere hår kvantitativt (for eksempel lengde, form, farge etc.), men hadde medført utfordringer for de andre kravene da det

finnes mange uten hår som svekker universaliteten og særpreg. I tillegg ville det også hatt dårlig permanens for de med hår da det vokser og vil kunne endre form og fasong relativt raskt.

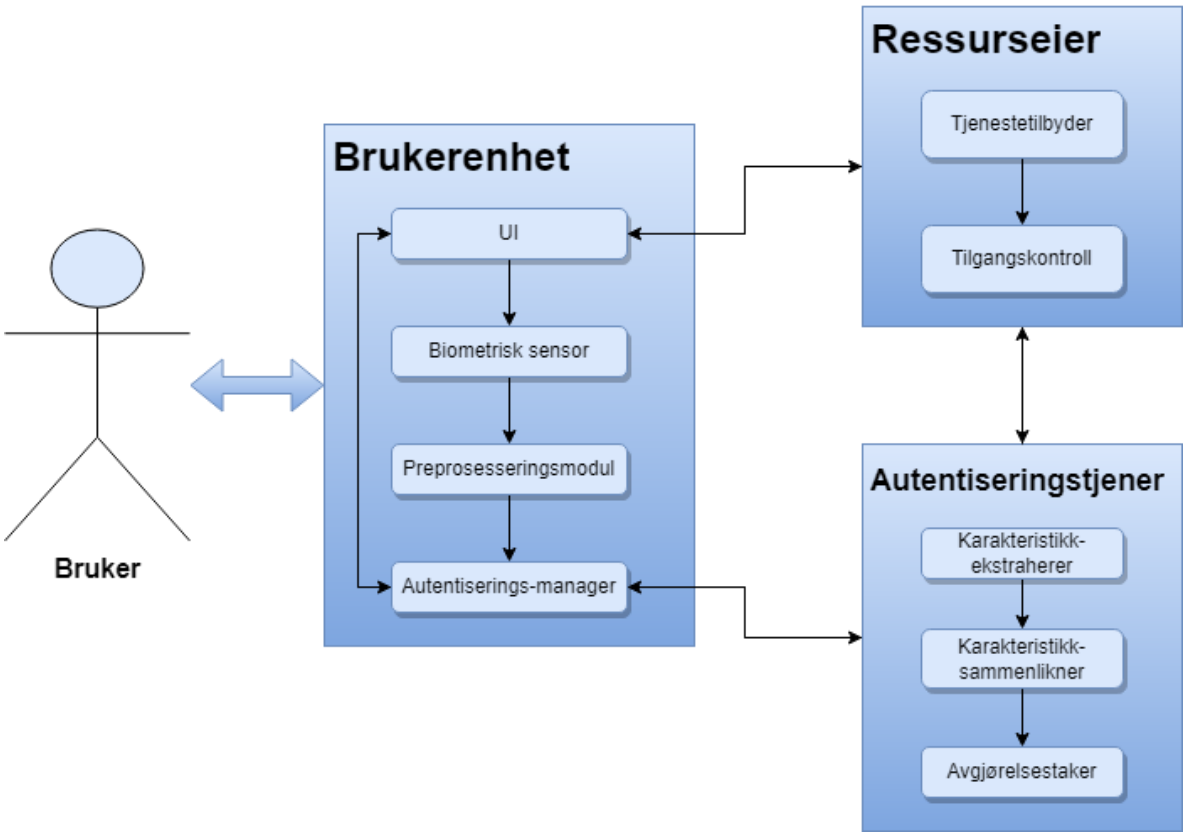
3.1 Autentiseringssystem

I brukerautentisering har man som nevnt en entitet med en tilhørende brukerkonto i en digital tjeneste som ønsker å bevise sin identitet slik at han eller hun får tilgang til sin bruker. Identitet i denne forbindelse er bruker-identiteten (bruker-ID). Denne bruker-IDen er en form for digital identitet som kan inkludere flere parametere, blant annet brukernavn eller andre attributter, som fysiologiske trekk med mennesket brukerkontoen tilhører. Verifisering av elementene som utgjør bruker-ID-en er nødvendig for å kunne referere til brukerkontoen som tilhører riktig menneske. For at dette skal være mulig, må man kunne skille ulike digitale identiteter fra hverandre, og det kreves dermed at en identitet har entydige, unike attributter. Det er her biometri gjør seg gjeldende. En biometrisk karakteristikk er en attributt som er unik for individet og gjør det mulig å verifisere korrekt individ for tilhørende bruker-ID. Samtidig er måling av disse biometriske attributtene ofte lettvint fra et brukerperspektiv og kan gjøres raskt, og er derfor praktisk å benytte for autentisering av en digital identitet.

En oversikt over hvordan et biometrisk autentiseringssystem kan organiseres er presentert i figur 2, hentet fra en artikkel av Rui og Yan (2019). Inkludert i denne oversiktsfiguren er brukerenheten, autentiseringstjeneren (i litteraturen kalt «Identity Provider») som kan verifisere brukeridentiteten, og ressurseieren («Relying party») som håndhever tilgangskontroll etter hva som ble gjort i autentiseringstjeneren.

Figur 2

Et eksempel på organisering av et biometrisk autentiseringssystem



Når brukeren forsøker å logge inn med sin identitet via sin enhet sendes en forespørsel fra autentiserings-manageren til autentiseringstjeneren. Autentiseringstjeneren sender så en autentiseringsforespørsel tilbake til autentiseringsmanageren i brukerenheten. Deretter vil brukerenheten gjøre måling av den biometriske modaliteten til brukeren og pre-prosessere denne informasjonen, før autentiseringstjeneren henter ut karakteristikkene («feature extraction») og sammenlikner det den får med hva som er lagret i databasen. På bakgrunn av dette gjøres det en avgjørelse på om målingen passer med standardmalen i databasen.

3.2 Autentiseringsfaser

Etableringsfase og bruksfase Det kan være nyttig å dele biometrisk autentisering-teknologien i to faser, registreringsfasen og bruksfasen (Jøsang, 2021; Kannavara & Bourbakis, 2009). Det må først, i etableringsfasen, etableres en standard-mal for den biometriske modaliteten til en bestemt bruker som lagres i en database. Her ekstraheres karakteristikker ved modaliteten som lagres sammen med andre identifikatorer, som for eksempel et unikt brukernavn. Denne standard-malen er originalen som benyttes når brukeren skal autentiseres senere i bruksfasen, der påfølgende målinger under autentisering sammenliknes med standardmalen.

I **bruksfasen** gjøres det flere målinger av den biometriske modaliteten og det blir beregnet et gjennomsnitt. man bryter ned modaliteten til karakteristikker som kan detekteres og måles. Hva disse karakteristikkene er avhenger modaliteten. For fingeravtrykk brytes den ned til ulike former for minutia. Dette er spesifikke punkter i fingeravtrykket, som der en linje i avtrykket deles eller slutter. Disse punktene danner altså et mønster man kan benytte til å representere fingeravtrykket med en binærkode. I bruksfasen vil det biometriske systemet måle modaliteten og ekstrahere de definerende karakteristikkene den får presentert. I en verifiserings-tilnærming vil mønsteret de ekstraherte karakteristikkene danner sammenliknes med det etablerte standardmalen. Denne sammenlikningen vil generere en skåring som reflekterer hvor lik målingen er det som er lagret som standardmal.

Biometriske modaliteter som ansikt og fingeravtrykk er brukt som autentikatorer. De er begge relativt lett tilgjengelig for måling, og er mulig å måle med brukerenheter som mobiltelefon. I sin presentasjon av deres nye iPhone X i 2017 hevdet Apple at der deres fingeravtrykksteknologi hadde en sannsynlighet på 1:50 000 at en annens fingeravtrykk kunne låse opp en annens iPhone, hadde deres nye ansiktsgjenkjenningsteknologi FaceID en sannsynlighet på 1:1 000 000. Det finnes flere ulike metoder for ansiktsgjenkjenning (Kannavara & Bourbakis, 2009; Rui & Yan, 2019). Et gjennombrudd skjedde i 2014 da et samarbeid mellom Facebook og Universitetet i Tel Aviv publiserte sitt «DeepFace»-system, en metode som benyttet «Deep Learning» for ansiktsgjenkjenning (Bud, 2018; Taigman et al., 2014). Denne metoden oppnådde en treffsikkerhet på 97.5%, som var en forbedring på mer enn 27% fra «state of the art» på den tiden. Denne teknologien ble videreført av blant annet Apple med sin FaceID. Her projiseres over 30 000 infrarøde punkter på ansiktet som analyseres og danner en dybdemodell, i tillegg tar et infrarødt kamera bilde av ansiktet, og disse blir sammen prosessert av et nevrale nettverk som lager en matematisk modell av ansiktet (Bud, 2018; *Om avansert Face ID-teknologi*, n.d.).

Med økt bruk av enheter man har på seg til enhver tid, som smartklokker, og som i tillegg foretar kontinuerlige målinger av fysiologiske aktiviteter ved individet som bærer dem, er det flere muligheter for å benytte noen av disse i en implementering av biometrisk autentisering (Liu et al., 2022). For eksempel kan hjerterytmen danne spesifikke mønstre som er tilgjengelig for bruk i autentiseringssystemer, og kan potensielt bli en viktig autentikator (V. Chandrashekhar et al., 2020). Chandrashekar et al. (2020) benyttet blant annet Apple Watch Series 5 for å hente

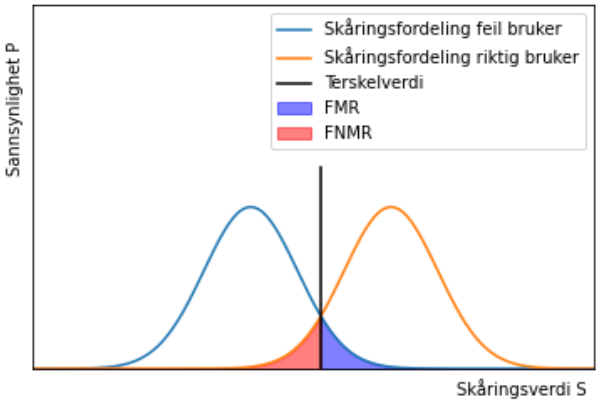
elektrokardiogram-signaler fra fem deltakere. Sammen med data fra to andre datasett så de hvordan ulike modeller presterte, med observerte «equal error rate» (EER) resultater som var under 3%.

Ved sammenlikning av den biometriske målingen og standardmalen gis som nevnt en skåring basert på hvor mye disse likner hverandre. For at det biometriske systemet skal fungere på en sikker måte er det viktig at riktige brukere blir verifisert og ikke-riktige brukere avvises. Dette omtales som det biometriske systemets presisjon. Når man evaluerer et biometrisk autentiseringssystem fokuserer man på fire mulige utfall ved autentiseringen, sann positiv, sann negativ, falsk positiv, falsk negativ (Jøsang, 2021). Ved sann positiv verifiseres korrekt bruker til sin tilhørende konto og ved sann negativ avvises en bruker som forsøker å verifiseres til en konto som ikke er dens egen. På samme måte er falsk positiv at en bruker blir verifisert til en konto som ikke er sin og falsk negativ at brukeren ikke blir verifisert til sin egen konto.

For å vurdere et biometrisk system sin kvalitet testes det på mange personer. Etter slike statistiske tester av et biometrisk system der et større antall feil- og riktige brukere inkluderes i testen får man to distribusjoner av deres skåringer, én for hver gruppe. Hvilke av de fire ulike utfallene nevnt i paragrafen over avhenger av en satt terskelverdi for hvor like målingen må være standardmalen. Et tenkt eksempel på slike statistiske distribusjoner visualiseres i Figur 3.

Figur 3

Statistiske distribusjoner for feil- og riktig brukere



Notat. Blå distribusjon viser skåringsfordeling for feil brukere til systemet, mens den oransje distribusjonen viser skåringsfordeling for riktige brukere. Y-verdiene (høyden på kurven) reflekterer sannsynligheten for at en enten feil eller riktig bruker får en skåringsverdi S. Lilla markering under kurven markerer andel brukere som blir feilaktig verifisert (FMR), rød markering viser feilaktig avvist (FNMR).

Ved å la mange teste det biometriske autentiseringssystemet kan man generere slike distribusjoner for ikke-autentiske og autentiske brukere som forsøker å autentisere seg til systemet. Når systemet sammenlikner den målingen en får ved forsøk på autentisering med korresponderende bruker lagret som standardmal gis det en skåringsverdi basert på hvor like disse er. Den horisontale x-linja i figurene 3 og 4 representerer denne skåringsverdien. Jo likere målingen er malen, jo høyere blir skåringsverdien. Men slik det er visualisert i figurene, er det ofte en overlapp mellom distribusjonene for autentiske og ikke-autentiske brukere. Dette kan skyldes at to målinger sjelden vil være helt identiske. Ulike faktorer som lysforhold, orientering av sensor i forhold til modaliteten eller naturlig variabilitet i modaliteten gjør at biometrisk autentisering ikke kan fungere på samme

måte som et passord, der det kreves en 100% match for vellykket autentisering. På grunn av denne variabiliteten, er det slik at det ved noen tilfeller vil forekomme at ikke-autentiske brukere blir feilaktig blir autentisert og autentiske brukere feilaktig ikke blir autentisert. Dette har tidligere i oppgaven blitt omtalt som henholdsvis, falsk positiv og falsk negativ. I litteraturen benyttes ofte «false match rate» (FMR) for raten av falsk positiv (antall falske positiver / totalt antall autentiseringsforsøk) og «false non-match rate» (FNMR) om raten av falske negativer (antall falske negativer / totalt antall autentiseringsforsøk). I og med at disse distribusjonene ikke er helt separert må det i et biometrisk autentiseringssystem være et mål som har som hensikt å balansere forekomsten av disse statistiske feilene som støtter sikkerhet på en best mulig måte. Dette målet er en terskelverdi som setter en grense for hvilken skåringsverdi som skal kvalifisere for godkjent autentisering. I Figur 3 er denne terskelverdien satt til å være i skjæringspunktet mellom de to distribusjonene, der FMR=FNMR. Dette er generelt antatt å være den mest optimale terskelverdien (Jøsang, 2021).

3.3 Angrep på biometriske system

Det finnes måter å bryte seg inn på en brukerkonto som ikke er ens egen ved å lure den biometriske autentisering, for personer som ønsker det. «Spoofing»-angrep er et begrep som dukker opp i litteraturen og omfatter slike forsøk på å stjele andres identitet. Generelt i forbindelse med biometri angår dette å forsøke å kopiere andres fysiologiske karakteristikker de benytter som autentikatorer. Kong et al. (2022) skisserer opp ulike «face presentation attacks» (FPA) som inkluderer, «print attacks» og angrep ved bruk av 3D-masker. Felles for disse er at begge forøker å lure det biometriske systemet ved å forsøke å etterlikne de fysiologiske karakteristikkene ved den identiteten de forsøker å stjele. Egenskaper ved det biometriske systemet for å detektere slike angrep omtales i litteraturen som «presentation attack detection» (PAD).

En annen form for angrep på biometriske systemer er «replay attacks» (Weaver, 2006). Her benyttes ikke fysiske etterlikninger av en biometrisk modalitet, men istedenfor kopieres den digitale representasjonen av biometriske målingen, slik at man unngår å benytte den faktiske fysiologiske enheten ved autentisering.

4 Diskusjon – Fordeler og utfordringer

I diskusjonsdelen vil informasjonen som er blitt presentert i delene over bli brukt til å vurdere fordeler og utfordringer ved biometrisk brukerautentisering.

4.1 Fordeler

Kanskje det mest interessante aspektet ved biometrisk autentisering er dets tydelige brukervennlighet. Målinger av en persons fysiologiske karakteristikker kan gjøres både raskt og er lett gjennomførbart for personen som ønsker å autentisere seg. Karakteristikker som er tilgjengelig for måling kan måles med enheter som stort sett alle til enhver tid har med seg i hverdagen. Dette inkluderer for eksempel mobiltelefon, personlige computere og/eller smart klokker. Brukeren kan la seg autentisere ved en hurtig måling av for eksempel ansiktskanning eller fingeravtrykkskanning som tillates av dagens teknologiske enheter.

Vi omgir oss med stadig flere enheter, med mer avansert teknologi, enn tidligere. Dette gir mulighet for måling av flere ulike modaliteter som kan benyttes i brukerautentisering. I og med at vi har både mobiltelefoner med utstyr til å kunne gjøre både ansikt- og fingeravtrykksverifisering, og smartklokker som måler hjerterytme etc. gir det muligheter for å kombinere flere modaliteter og dermed gjøre autentiseringen enda sikrere. Dersom man i tillegg bruker andre autentiseringsfaktorer som PIN eller passord vil slik flerfaktor-autentisering redusere

sannsynligheten for feil/falsk autentisering. For eksempel viste en studie av Chandrashekar et al. (2020) at dagens Apple Watch kan måle elektrokardiogram-signal med en slik effektivitet at det potensielt kan benyttes som en kontinuerlig biometrisk autentikator.

FIDO Alliance har uttalt bruk av passord alene er en stor sikkerhetstrussel i dag (Glavin, 2022). Dette begrunnes med at passord har sårbarheter som at de kan glemmes, stjeles, i tillegg til at de kan være for svake til å forhindre sikker autentisering. Phishing og sosial manipulasjon som metoder for å stjele autentikatorer blir en stadig større trussel (ForgeRock, 2022; Skatteetaten, 2022; Statistisk sentralbyrå, 2022). En av løsningene som blir foreslått til de potensielle sikkerhetstruslene brukerautentisering som kun benytter seg av passordbeskyttelse medfører er flerfaktor-autentisering (Jøsang, 2021). Ved bruk av flere autentiseringsfaktorer blir autentiseringen sikrere da sannsynligheten for falske positiver reduseres, og kan representeres ved å vurdere sannsynligheten for falsk positiv med faktorene hver for seg. Kombinert blir sannsynligheten for falske positiver med flere faktorer produktet av disse sannsynlighetene som er mindre enn hver av de isolert. FIDO Alliance inkluderer både biometriske autentiseringsfaktorer i tillegg til eksterne autentikatorer, som sikkerhetsnøkler ("FIDO Alliance Specifications Overview," n.d.). Dette bidrar til at private personer får en sterkere beskyttelse av sine data i digitale tjenester som i større grad enn tidligere består av viktig informasjon. Flere finansielle og statelige tjenester for eksempel eksisterer nå digitalt (Jøsang, 2021).

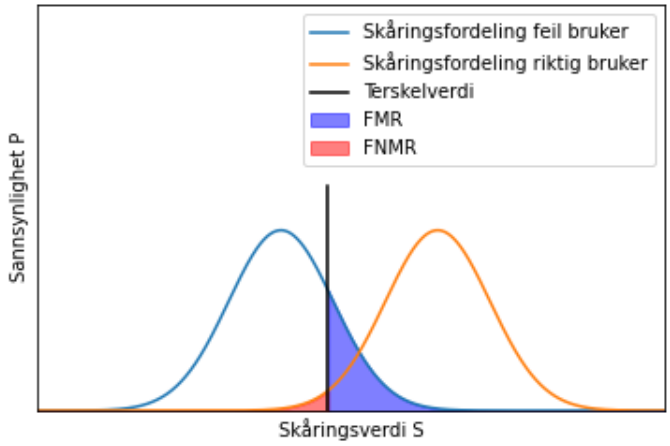
4.2 Utfordringer

En utfordring ved biometriske systemer er sensitivitet for falske positiver. Dette kan håndteres ved å endre terskelen for hvor sensitiv sammenlikningen mellom standardmalen og målingen som tas ved autentisering skal være. Ved lav terskelverdi risikerer man å øke andel FMR, men samtidig også redusere FNMR, slik det er visualisert i figur 4 a). Dette kan føre til betydelig sikkerhetsrisiko da det betyr at sannsynligheten for at personer som ikke tilhører brukerkontoen feilaktig blir autentisert. Dette vil igjen kunne få store konsekvenser avhengig av hva denne uvedkomne får tilgang til av ressurser. For eksempel kan dette dreie seg om store økonomiske tap om det er autentisering til finansielle tjenester. Visualisering av hvordan terskelverdien påvirker utfallet av autentiseringen vises i figur 4.

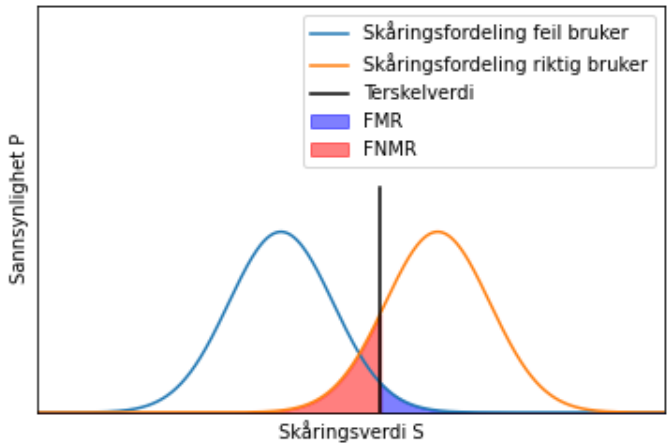
Figur 4.

Statistiske distribusjoner for feil- og riktige brukere med ulik terskelverdi

a)



b)



Notat. Her er lik distribusjon som i Figur 3, men med ulike terskelverdier. a) viser hvordan FMR øker og FNMR reduseres med lavere terskelverdi, mens b) viser hvordan FMR reduseres og FNMR øker ved høyere terskelverdi.

I Figur 4 ser vi hvordan terskelverdien påvirker det biometriske autentiseringssystemet. Settes det lavt, som beskrevet i paragrafen over, risikerer man at flere som ikke skal ha tilgang kan få tilgang, og eventuelt også gjøre «spoofing»-angrep enklere å lykkes med. Settes den derimot høyt (som i figur 4b) ser vi at FNMR øker. Dette vil medføre betydelig påvirkning på brukeropplevelsen, og dermed også et av aspektene ved de positive sidene ved biometrisk autentisering – dets brukervennlighet. Dersom en bruker opplever at for eksempel autentiseringen fungerer 1 av 4 ganger er det legitimt å anta at personen ønsker å ikke benytte seg av autentiseringen. Som nevnt er et av de positive sidene ved biometrisk autentisering brukervennligheten. Denne brukervennligheten kan gjøre at brukeren velger å benytte flerfaktorautentiserings-metoder, istedenfor kun ett passord som tidligere nevnt kan medføre potensiell risiko. Terskelverdien til et biometrisk system er derfor ekstremt viktig. Den skal både sørge for en sikker autentisering, der falske positiver forekommer minimalt, samtidig som den ikke kan settes så høyt at det går utover brukervennligheten.

Målet med et biometrisk autentiseringssystem er å verifisere legitime brukere, samtidig som det skal hindre illegitime angripere tilgang til ressursen de forsøker å autentisere seg til. Alle de ulike biometriske modalitetene er sårbare for falske positiver, som dette siste tilfellet representerer. «Spoofing»-angrep, der illegitime entiteter forsøker å benytte falske og kopierte biometriske autentikatorer for å logge seg inn hos andres brukere, mot biometriske systemer som benytter ansiktsgjenkjenning kan for eksempel inkludere bilder av de «ekte» fysiologiske karakteristikkene. Dette har i senere tid ført til metoder som inkluderer dybdeinformasjon, altså 3D-modeller istedenfor 2D-modeller, i autentiseringen. Apple sin FaceID benytter for eksempel infrarøde punkter sammen med spesialiserte sensorer for å etablere en 3D-modell av ansiktet som autentiseres (Bud, 2018). Men også 3D-modeller er vist å kunne konstrueres, også kun fra 2D-bilder, for å benytte som «spoofing» (Xu, 2016). Som i andre grener av informasjonssikkerhet er det en kontinuerlig kamp mellom angreps- og beskyttelsesmekanismer, og dersom en angriper virkelig vil, og har tilstrekkelig ressurser, vil det være mulige å forbigå et biometrisk autentiseringssystem.

Til slutt er et aspekt, som det er nødvendig å inkludere i en diskusjon om bruk av biometriske metoder, personvern. Ikke bare fungerer biometrisk autentisering for beskyttelse av sensitiv informasjon, den biometriske autentikatoren er i seg selv privat og sensitiv form for informasjon. Biometrisk informasjon er privat. Konsekvenser av angrep på biometriske systemer eller databaser med biometrisk informasjon kan medføre krenkelser av privatlivet, og lagring av biometrisk informasjon stiller derfor særlige krav til konfidensialitet.

5 Konklusjon

Dagens personlige enheter er utstyrt med teknologi som gjør det mulig å gjennomføre avanserte målinger av fysiologiske karakteristikker ved personene som eier og bærer disse enhetene. I tillegg ser vi en økende digitalisering av vesentlige tjenester, kombinert med store forekomster av trusler mot digital informasjonssikkerhet. Dette setter søkelyset mot metoder for hvordan brukere kan benytte slike digitale tjenester på en sikker måte. En måte å øke sikkerheten av bruk av digitale tjenester på er ved flerfaktor-autentisering. Her er bruk av biometriske autentikatorer en potensielt viktig aktør. Denne oppgaven har gjennomgått relevant litteratur for biometrisk autentisering, og forsøkt å gi en bedre forståelse av hva det er, hvordan det kan benyttes for å gjøre brukerautentisering sikrere, og i tillegg undersøkt fordeler og utfordringer ved biometriske metoder for brukerautentisering. Som vi har sett kan biometriske metoder inkluderes i systemer for flerfaktor-autentisering for å bedre brukerautentisering. Samtidig er det viktig å være klar over dets sårbarheter, og at det ikke brukes alene som den eneste metoden for brukerautentisering. Biometriske metoder er brukervennlige løsninger som dagens teknologi gjør enda mer tilgjengelig, men det må inkorporeres i systemer som benytter flere autentikatorer.

6 Bibliografi (APA 7th ed)

Bud, A. (2018). Facing the future: The impact of Apple FaceID. *Biometric Technology Today*, *2018*(1), 5–7. https://doi.org/10.1016/S0969-4765(18)30010-9

FIDO Alliance Specifications Overview. (n.d.). *FIDO Alliance*. Retrieved November 1, 2022, from https://fidoalliance.org/specifications/

ForgeRock. (2022). *2022 ForgeRock Consumer Identity Breach Report | ForgeRock*. https://www.forgerock.com/resources/analyst-report/2022-forgerock-consumer-identity-breach-report

Glavin, L. (2022, May 5). Apple, Google and Microsoft Commit to Expanded Support for FIDO Standard to Accelerate Availability of Passwordless Sign-Ins. *FIDO Alliance*.

https://fidoalliance.org/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard-to-accelerate-availability-of-passwordless-sign-ins/

ISO. (2018). *ISO/IEC TR 24741:2018(en), Information technology—Biometrics—Overview and application*. https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24741:ed-2:v1:en

Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, *14*(1), 4–20.

Jøsang, A. (2021). *Informasjonssikkerhet: Teori og praksis*. Universitetsforlaget.

Kannavara, R., & Bourbakis, N. (2009). A Comparative Survey on Biometric Identity Authentication Techniques Based on Neural Networks. In *Biometrics* (pp. 47–79). https://doi.org/10.1002/9780470522356.ch3

Kong, C., Wang, S., & Li, H. (2022). *Digital and Physical Face Attacks: Reviewing and One Step Further* (arXiv:2209.14692). arXiv. http://arxiv.org/abs/2209.14692

Liu, S., Shao, W., Li, T., Xu, W., & Song, L. (2022). Recent advances in biometrics-based user authentication for wearable devices: A contemporary survey. *Digital Signal Processing*, *125*, 103120. https://doi.org/10.1016/j.dsp.2021.103120

Merriam-Webster. (n.d.). *Authentication*. Retrieved October 25, 2022, from https://www.merriam-webster.com/dictionary/authentication

Økt digitalisering i offentlig sektor som følge av koronapandemien. (2021, May 6). ssb.no. https://www.ssb.no/teknologi-og-innovasjon/artikler-og-publikasjoner/okt-digitalisering-i-offentlig-sektor-som-folge-av-koronapandemien

Om avansert Face ID-teknologi. (n.d.). Apple Support. Retrieved October 27, 2022, from https://support.apple.com/no-no/HT208108

Rui, Z., & Yan, Z. (2019). A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification. *IEEE Access*, *7*, 5994–6009. https://doi.org/10.1109/ACCESS.2018.2889996

Skatteetaten. (2022, March 10). *Nye tall: 150 000 nordmenn har opplevd ID-tyveri de siste årene*. Skatteetaten. https://www.skatteetaten.no/presse/nyhetsrommet/nye-tall-150-000-nordmenn-har-opplevd-id-tyveri-de-siste-arene-/

Statistisk sentralbyrå. (2022, May 6). *Forsøk på identitetstyveri er fortsatt det mest utbredte IKT-sikkerhetsproblemet*. SSB. https://www.ssb.no/teknologi-og-innovasjon/informasjons-og-kommunikasjonsteknologi-ikt/statistikk/digitalisering-og-ikt-i-offentlig-sektor/artikler/forsok-pa-identitetstyveri-er-fortsatt-det-mest-utbredte-ikt-sikkerhetsproblemet

Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. (2014). DeepFace: Closing the Gap to Human-Level Performance in Face Verification. In *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*. https://doi.org/10.1109/CVPR.2014.220

V. Chandrashekhar, P. Singh, M. Paralkar, & O. K. Tonguz. (2020). Pulse ID: The Case for Robustness of ECG as a Biometric Identifier. *2020 IEEE 30th International Workshop on Machine Learning for Signal Processing (MLSP)*, 1–6. https://doi.org/10.1109/MLSP49062.2020.9231814

Weaver, A. C. (2006). Biometric authentication. *Computer*, *39*(2), 96–97.

Xu, Y. (2016). *Virtual U: Defeating Face Liveness Detection by Building Virtual Models From Your Public Photos*. 17.