Institutt for informatikk

Mange veier inn – en studie av alternative innloggingsmekanismer

Hans Joachim Desserud

23. mai 2011

Sammendrag

Passord er den mest brukte mekanismen for innlogging, enten det gjelder datamaskiner, nettsteder, tjenester, og så videre. Per i dag blir de fleste stadig medlem av flere nettsteder som gjør at vi må huske flere passord til forskjellige steder. Hvis vi har for vanskelige passord blir de umulig å huske alle, men er de for enkle, vil andre enkelt gjette seg frem til dem.

Dermed blir det mer aktuelt med alternative autentiseringsmekanismer, for å erstatte eller tilby et alternativ til passord. For brukere som foretrekker eller bedre husker bilder er det kanskje en løsning, mens andre vil logge inn ved å svare på personlige spørsmål. I tillegg finnes det flere muligheter, men få av dem er i utstrakt bruk.

For å kunne foreslå alternative mekanismer istedenfor eller i tillegg til passord, er det først nødvendig å vite hvilke som finnes. En del har blitt foreslått og tatt i bruk, mens andre fortsatt har enkelte problemer og er under utvikling. Siden brukerne skal forholde seg til mekanismene er det viktig å finne ut hvilke de foretrekker og om det er problemområder som bør utbedres. Her vil vi teste ut fem mekanismer med en liten brukergruppe for å se hvilke de foretrekker og hvordan de vurderer dem i forhold til hverandre.

Til slutt er oppfatningen og det bildet brukerne har av mekanismene en viktig detalj. Sikkerheten er der for å beskytte mot ulike trusler, men hvilke trusler ser brukerne for seg er mest aktuelle? Har de et reelt bilde på farene der ute, eller er det potensielt områder de har oversett?

Målet med oppgaven er å se på hvilke mekanismer som finnes, hvordan de fungerer i praksis, og hvilke modeller brukere har rundt innlogging og potensielle trusler. Selv om alternative mekanismer finnes, må de testes ut for å se hva brukere synes om dem, om de er forståelige og hvordan brukere liker dem i forhold til tradisjonelle passord.

Forord

Dette er en kort masteroppgave i Informatikk, som har blitt skrevet våren 2011 ved Institutt for Informatikk ved Universitetet i Oslo. Oppgaven har fokus på aspekter innenfor sikkerhet og design, og jeg føler jeg har lært mye innenfor begge områder gjennom arbeidet med oppgaven.

Gjennom våren har jeg lest en lang rekke artikler og noen bøker for å finne ut mer om innlogging og autentisering. Samtidig har jeg fått lov til å være med på møtene til forskningsprosjektet e-Me og fått et innsyn i hva de jobber med. Jeg fikk også lov til å være med på brukerundersøkelser de arrangerte som ga meg interessante funn jeg kunne bruke i oppgaven min.

Jeg ønsker å takke alle involverte i prosjektet e-Me som lot meg få være med på møter og brukertester. Jeg vil også takke veilederen min, Jo Herstad, som har bistått med diskusjoner og forslag til relevante bøker og artikler.

Hans Joachim Desserud
Mai 2011

Innhold

1 Introduksjon

1.1 Innledning

Vi må i stadig større grad huske på passord, PIN-koder og andre hemmeligheter. De er nødvendige for å få tilgang til datamaskiner, mobiltelefoner, tjenester som bank, forsikring og et ukjent antall nettsteder vi er medlem av. Er det andre mekanismer enn de som blir benyttet i dag, som kan gjøre det enklere å huske hvordan vi logger oss inn de forskjellige stedene?

Essensen av sikkerhet kan sees på som å sikre tilgangen til noe (en ressurs), ved å kunne sørge for at noen har tilgang mens andre ikke har det. Formålet med sikkerhet er å kunne ha en oversikt over disse to gruppene og kunne skille mellom dem. Som en følge av dette, kan innlogging sees på som et av de viktigste aspektene av sikkerhet. Hvis innloggingen feiler, hjelper det ikke hvilke andre tiltak som finnes, siden det ikke en gang er en viss kontroll over hvem som har tilgang. Sikkerhet, som en kjede, er ikke sterkere enn sitt svakeste ledd.

Historisk sett har det vært mange og varierte mekanismer for å sikre tilgang og stenge uvedkommende ute. En av de mest utbredte er å kunne låse noe, og ha en nøkkel for å låse det opp eller igjen. Et godt eksempel er en dør. Låsen på en dør skal hindre uvedkommende adgang, mens de som har en nøkkel skal kunne komme seg inn eller ut. Å låse huset eller bilen er situasjoner hvor mekanismen som blir benyttet er klar og farene rundt er kjent. Vi kunne spart mye tid på å kunne la dørene stå åpne fremfor å låse dem, men de fleste er klar over at andre vil utnyttet ulåste ytterdører. Ulempen med å bruke et par sekunder ekstra mot å være tryggere på at tingene sine fortsatt er der når vi kommer hjem igjen gjør det til et enkelt valg. I dette tilfellet har brukere avfunnet seg med at sikkerhetsløsningen er fornuftig og hensiktsmessig i forhold til det ekstra arbeidet eller tiden det utgjør.

Når en bruker benytter et dataprogram eller -system, er det fordi de ønsker å bruke det som et verktøy, ikke nødvendigvis sette seg inn i hvordan den underliggende teknologien fungerer. Likedan som telefonen brukes til å kommunisere med andre, uten at de fleste har oversikt over detaljer som mikrofonen vi snakker i eller nettverket informasjonen sendes gjennom. De fleste brukere har bestemte arbeidsoppgaver eller andre ting de skal gjøre og alt som ikke hjelper dem utføre den oppgaven er enten uviktig eller i verste fall et hinder. For de fleste er det trolig overkommelig å logge seg inn på sin maskin i likhet med at vi låser opp ytterdøra når vi kommer hjem. Sikkerheten har en åpenbar verdi; uvedkommende hindres adgang ved å benytte seg av maskinen. Dessverre er det ofte slik, at det ikke holder med

å logge seg inn kun en gang, det er ofte nødvendig å logge seg inn en gang til for å få tilgang til spesielle systemer, eller en forskjellige systemer. Disse systemene kan ha forskjellige grader av sikkerhet, men er alle viktige nok til at brukeren må bevise at han eller hun virkelig har tilgang til å bruke det.

Vi kan tenke oss at en enkelt bruker benytter seg av kanskje 10-20 forskjellige systemer med ulik grad av sikkerhet som hver har sine krav om passord. Noen har minimumslengde, mens andre andre skal inneholde spesialtegn, tall, kombinasjon av store og små bokstaver, de kan ikke være like noen av passordene brukeren har benyttet tidligere. I tillegg skal de byttes med jevne mellomrom, noen så ofte som en gang i måneden, og det er heller ikke lov å benytte det samme passordet på tvers av de forskjellige tjenestene. I teorien en god plan for å sikre gode, unike passord som vil gjøre det vanskeligere for uvedkommende å misbruke systemet. Dessverre fører det samtidig til at det blir mer tungvint for brukere å benytte seg av systemene i hverdagen. Først og fremst er brukerene ute etter å gjennomføre de arbeidsoppgavene de har, ikke pugge forskjellige passord hele dagen. Selvom enkelte vil klare å holde styr på de forskjellige vil det ta mye energi. På et tidspunkt oppdager enkelte at istedenfor å lære seg samt huske et vanskelig passord som sjelden brukes, er det letter å notere det på en lapp og skrive det av de få gangene det er nødvendig. Brukeren får gjort jobben sin, i henhold til regelverket benyttes et sterkt passord, men sikkerheten lider. Det er viktig å se at alt som hindrer brukeren i å gjøre det han eller hun vil, kan bli sett på som hindringer og omgås. Brukere vil i stor grad ta snarveier når det kommer til sikkerhet fordi det ikke bidrar til arbeidsoppgavene.

Etter at verdensveven (World Wide Web) ble introdusert på begynnelsen av 1990-tallet, har den bredt om seg, og de fleste er per idag medlem av et stadig økende antall nettsteder. Det vanligste måten å logge seg inn på nettsteder er å oppgi et brukernavn og passord. Ved hjelp av denne mekanismen er det mulig å skille mellom brukere som har tilgang og alle andre. For de fleste tjenester er det naturlig at brukerne har registrert seg for at tjenesten skal kunne lagre informasjon for brukerne, der de kan ha sine egne innstillinger og lignende uten at andre får tilgang. Tjenesten på sin side blir i stand til å skille mellom registrerte medlemmer og besøkende som ikke er registrerte. Siden de fleste nettsteder krever medlemskap, og det kommer stadig nye nettsteder der vi registrerer oss, ender brukere opp med flere brukernavn og passord å holde styr på enn tidligere. For at brukere skal være i stand til å kommunisere med andre, krever de fleste nettsteder at brukere registrerer seg og logger inn for å kunne kommunisere og dele informasjon med andre brukere. I slike situasjoner er det viktig at brukergrupper ikke ekskluderes, og blir utestengt fra nettstedet som følge av at de vil ha problemer innloggingen.

Passord har blitt brukt i lengre tid, og var en kjent mekanisme for å

avgjøre om brukere var den de ga seg ut for å være. I begynnelsen var det også overkommelig, siden vi var medlemmer på et eller et begrenset antall nettsteder. Men tiden har gått, og det har kommet stadig flere nettsteder for ulike interesseområder, og systemer vi skal ha tilgang til i forbindelse med jobb, utdanning og andre sammenhenger. Dette gjør at brukere får en større mengde passord å huske. Selv om bruk av passord er utbredt, har det enkelte svakheter. Svake passord kan lett gjettes, men for kompliserte kan føre til at brukeren glemmer det. Brukere som deltar på større mengder nettsteder og sosiale medier vil kunne ende opp med en større mengde passord de må gå rundt å huske til de forskjellige tjenestene.

Mens flesteparten vil ha problemer med å huske en større mengde passord, kan enkelte ha problemer med selve mekanismen. Brukergrupper som dysleksikere problemer med å huske passord og skrive dem korrekt, personer med motoriske problemer vil ha problemer med å skrive lengre passord korrekt, noen grensesnitt for innlogging er umulig å bruke for blinde og svaksynte og andre brukergrupper har sine problemer. Ved å kunne tilby alternative innloggingsmekanismer vil vi kunne legge bedre til rette også for disse gruppene. Samtidig kan det bidra til at den jevne bruker får det enklere ved å ha muligheten til å kunne benytte andre mekanismer enn å huske en rekke passord.

1.2 Motivasjon

Jeg oppfatter innlogging som en viktig, men kanskje ofte oversett del av interaksjonen mellom brukere og informasjonssystemer. Til tross for at prosessen er en integrert del av bruken av datamaskiner og ofte en forutsetning for å kunne benytte de fleste systemer. Ved å logge seg inn på enten en datamaskin, nettside eller mobile enheter oppgir vi hvem vi er og blir godkjent som en bruker. Dette blir kanskje ubevisst en prosess som blir sett på som en automatisk og liten del av bruk av datamaskiner, men er fortsatt en viktig del av interaksjonen vi har med IT-systemer.

Nesten samme hva vi gjør, fra å slå på maskinen til å få tilgang til e-post eller andre tjenester på nett, er innlogging en del av prosessen. Hovedsaklig blir brukernavn og passord benyttet. Det er mange aspekter å ta hensyn til og mange problemstillinger som kan belyses. Et interessant aspekt er at selv om det er en prosess som vil berøre alle registrerte brukere for et nettsted, blir det kanskje lagt liten vekt på hvordan innloggingen skal utformes eller legges til rette. Passord har etablert seg godt, og regnes som en de facto standard. De fleste som utvikler nye tjenester tar i bruk denne mekanismen og kopierer hvordan andre tjenester håndterer innlogging. Sannsynligvis skjer dette valget uten at utviklere og designere tenker stort over hvordan innlog-

gingsprosessen faktisk fungerer og hvilke alternativer som er tilgjengelige.

Jeg har lenge vært opptatt av sikkerhet og webløsninger, og synes derfor det vil være interessant å studere hvilke løsninger og muligheter det er for å kunne logge seg inn. En løsning jeg har lagt merke til er Single sign-on, som gjør det mulig å logge inn flere steder med samme brukerinformasjonen. Dette er en løsning som har blitt tatt i bruk i større grad i det senere, og er en interessant måte å forholde seg til autentisering på. Jeg er også interessert i selve innloggingen og hvilke mekanismer som kan tas i bruk der. Gjennom arbeidet med denne oppgaven har jeg oppdaget enkelte alternative mekanismer for innlogging, både som jeg har sett referanser til tidligere eller ikke, som jeg synes det var interessant studere nærmere.

Etter som både datamaskiner, mobile enheter og forskjellige webtjenester stadig blir en større del av hverdagen til mange, er det interessant å ikke bare se på mulighetene med teknologien, men også hvor stor forståelsen er. Veldig mye blir tatt i bruk uten at det blir gitt noen god forklaring på hvordan ting fungerer under panseret. Det er selvfølgelig ikke et krav at brukere skal kunne kjenne til den minste lille detalj for å kunne bruke noe, og det vil være umulig å lære seg alt i løpet av et liv. Likevel kan det komme godt med å ha generell kunnskap til hvordan noe er bygget opp, og kunne danne seg en forståelse av hvordan et system kan brukes og hvordan det fungerer. Det hjelper både i møte med lignende systemer eller oppgaver i fremtiden eller for å kunne finne årsaken hvis noe går galt. Jeg tror hvordan vi bruker ting, henger veldig mye sammen med hva vi tror de kan gjøre og hvilke resultater vi har fått tidligere. Særlig sikkerhet er et område hvor det er veldig vanskelig å avgjøre hvor godt vi kjenner systemet, og om vi faktisk er beskyttet mot de aktuelle truslene på en effektiv måte.

I kurset Mobile Informasjonsystemer skrev jeg sammen med tre andre om metoder for autentisering for mobile enheter. Jeg synes oppgaven var interessant og jeg ble mer interessert i prosessen rundt autentisering og forskjellige mekanismer som kan benyttes. I sammenheng med den oppgaven fikk jeg også innsyn i flere ulike mekanismer for å logge seg inn, som jeg ønsket å se mer på senere. Fokus da var spesifikt mot mobile enheter, og så på hvilke muligheter og begrensninger som spiller inn. For masteroppgaven ønsket jeg å se videre på mekanismer for innlogging.

Jeg anser innlogging som et godt eksempel for å beskrive konseptet sikkerhet, siden det er den delen av sikkerhet de fleste av oss har et forhold til. Ved å skru på datamaskinen oppgir vi et passord, på mobiltelefonen en PIN-kode for å komme inn. Videre kobler vi oss opp mot diverse nettsteder eller andre tjenester der vi igjen må logge oss inn for å få tilgang. Sånn sett er kanskje innlogging den delen av sikkerhet vi blir oftest utsatt for og som vil være lett å kjenne igjen. Det er selvfølgelig andre, like viktige aspek-

ter ved sikkerhet. De underliggende kryptografiske systemene, brannmurer, malware, sikkerhetskopier er bare noen av bitene som utgjør sikkerhet. Selv om de andre aspektene også er interessante, er det innloggingen jeg har lyst til å se nærmere på. Det er kanskje den delen som er mest i bruk, selv om den kanskje ikke legges merke til som en del av sikkerheten for et systemet. I tillegg til sikkerhetsaspektet, synes jeg det ville være interessant å se fra brukerenes perspektiv. Hvordan brukere oppfatter ulike mekanismer, og hva de foretrekker vil kunne påvirke hvilke mekanismer de velger seg, som er valg designere bør ta stilling til i arbeidet med et nytt system.

For at alle skal kunne benytte nettsteder og tjenester, er det et stort fokus på å legge til rette i forhold til universell utforming. Samtidig blir passord automatisk tatt i bruk til innlogging, selve innloggingsprosessen blir knapt nevnt. Mye av grunnen kan være at innloggingen er et ledd i interaksjonen med tjenesten som blir lett oversett eller tatt for gitt. Men for enkelte brukergrupper er det kanskje her det største problemet befinner seg. Krav om avanserte passord som er vanskelige å huske, former for innlogging som er vanskelige å benytte fra skjermlesere eller punktskrift. Hvis brukere i utgangspunktet ikke er i stand til å logge inn på tjenesten hjelper det lite samme hvor mye den er lagt opp mot forskjellige behov.

1.3 Problemstilling

Innenfor autentiseringsmekanismer og innlogging er det flere aspekter som kan være interessante å se nærmere på. Det finnes forskjellige mekanismer for å logge seg inn som tilbyr ulike grader av sikkerhet og tilgjengelighet. Det finnes også enkelte mekanismer som er mer egnet for spesifikke systemer og brukergrupper i forhold til andre. Et gjennomgående tema er at brukere i stadig større grad får større antall steder og tjenester der de er registrert å forholde seg til, og innloggingsinformasjon de må håndtere. I forhold til denne utviklingen er det relevant å ta for seg hvilke mekanismer som kan benyttes som alternativer til tradisjonelle passord.

I denne oppgaven vil jeg se på noen av de forskjellige mekanismene for innlogging som finnes per i dag. Passord har lenge vært de facto standard for innlogging, men det er mulig andre mekanismer kan tilbys som et alternativ. Spesielt med tanke på brukere med andre behov, f.eks. dyslektikere eller eldre. En annen viktig element er å se på mer på hvilke muligheter alternative mekanismer har, men også hvilke problemer som er knyttet til de ulike mekanismene. Jeg ønsker å se på de ulike mekanismen på to nivåer. For det første studere de ulike mekanismene slik de er og hvilke alternativer som finnes, og for det andre se på hvordan brukere forstår mekanismene. I hovedsak vil oppgaven ta for seg følgende problemstillinger:

1. Hvilke ulike autentiseringsmekanismer er i bruk eller kan benyttes per i dag?

2. Hvordan fungerer et utvalg av av disse mekanismene under utprøving med brukere i praksis?

3. Hvilke mentale modeller har brukere for de forskjellige mekanismene og trusselbildet rundt?

1.3.1 Hvilke ulike autentiseringsmekanismer er i bruk eller kan benyttes per i dag?

Jeg ønsker å kartlegge hvilke forskjellige autentiseringsmekanismer som finnes og kan benyttes per i dag. Å gi et fullstendig bilde av alle mekanismer som har blitt foreslått blir for omfattende, så jeg begrenser meg til et representativt utvalg av løsninger som har blitt benyttet i en eller annen grad. I tillegg tas det med enkelte lovende mekanismer som fortsatt er under utvikling eller på forskningsstadiet. Passord er som kjent den mest brukte autentiseringsmekanismen, men hvilke andre mekanismer finnes som kan benyttes? Spesielt vil oppgaven se på hvilke mekanismer som kan være mer rettet mot enkelte brukergrupper og øke tilgjengeligheten for disse.

Det er trolige at mekanismene har ulike fordeler og ulemper. Passord er i utgangspunktet vanskelig for andre å gjette, men kan bli vanskelig å holde orden på hvis de blir for kompliserte. Det er også andre svakheter, og det kan tenkes andre mekanismer har andre svakheter. Sett i forhold til passord, er det mulig å kort skildre enkelte av svakhetene som utmerker seg ved de ulike mekanismene, som bør tas hensyn til ved implementering eller i verste fall ekskluderer mekanismene for bruk.

For å få en oversikt over de ulike mekanismene vil jeg se på hvilke mekanismer som har blitt foreslått og hvilke som er i daglig bruk. Interaksjonen og bruken av datamaskiner har endret seg radikalt siden de først ble innført, og det er dermed relevant hvordan disse endringene har påvirket innloggingsprosessen. Det vil også være aktuelt å se fremover, for hvilke nye metoder for interaksjon som kan gjøre seg gjeldende og hvilke mekanismer som kan erstatte eller benyttes i tillegg til passord. Det kanskje mest interessante aspektet blir å se om de alternative mekanismene kan benyttes, eventuelt hvilke hindringer og problemer bør utbedres før de blir tatt i bruk.

1.3.2 Hvordan fungerer et utvalg av av disse mekanismene under utprøving med brukere i praksis?

Hvis målet er å finne autentiseringsmekanismer som kan fungere som et alternativ til eller erstatte passord, er det viktig at det faktisk er mulig å bruke de ulike mekanismene. Ved å gjennomføre en brukertest med enkelte alternative mekanismer, vil det være mulig å identifisere hvilke mekanismer som fungerer som forventet, og hvilke som har mangler eller som brukerene har problemer med. Kombinert med brukernes oppfattelse og vurdering av mekanismene, er det mulig å si noe om hvilke brukerne foretrekker. Hvilke mekanismer brukerne foretrekker eller har problemer med, er interessant i vurderingen av hvilke mekanismer som kan benyttes.

Under testingen av mekanismene, har jeg valgt å fokusere på enkelte brukergrupper, for å bedre kunne bedømme hvor godt de forskjellige mekanismene er tilrettelagt disse gruppene. I oppgaven ønsker jeg å se på hvordan de ulike mekanismene er tilrettelagt brukere med ulike behov, som for eksempel eldre og dyslektikere. En viktig del er å kunne se på hvordan brukerne forstår mekanismene, og i hvor stor grad de kan raskt sette seg inn i og ta de i bruk. I tillegg vil jeg se litt på hvilke problemområder de forskjellige mekanismene har for brukergruppene som tester dem.

Selve testen vil basere seg på en prototype som inneholder ulike autentiseringsmekanismer. De vil bli testet ut av en mindre gruppe brukere. Gjennom testen vil jeg være med og observere hvordan brukerne forholder seg til de alternative mekanismene, og eventuelle problemer som oppstår underveis. Testpersonene vil også bedømme de ulike mekanismene og komme med tilbakemelding på hvilke de foretrakk og hvorfor. Siden testpersonene er valgt fra spesifikke brukergrupper, vil det være vanskelig si noe generelt i forhold til resten av befolkningen. Dette er heller ikke intensjonen, formålet er først å fremst å se hvordan brukerne håndterer de forskjellige mekanismen, hvilke som virker lovende og hvilke som har problemområder som bør utbedres.

1.3.3 Hvilke mentale modeller har brukere for de forskjellige mekanismene og trusselbildet rundt?

Mentale modeller beskriver de modellene brukerne konstruerer i forhold til hvordan de oppfatter et system og hvordan de antar det fungerer. De mentale modellene er viktige, ved at de påvirker hvordan brukere oppfatter systemet og bruken av det. For at brukeren bedre skal forstå systemet er det viktig at det fungerer slik brukerne forventer seg, og at det klarer å formidle hva som er forventet adferd.

Gjennom designet av systemet vil designeren benytte seg av elementer

som metaforer og tilbakemeldinger for å forme en ønsket mental modell av systemet. Hvis designeren lykkes, vil brukeren danne seg en mental modell som samsvarer med hvordan systemet oppfører seg. Hvis det derimot oppstår ulikheter mellom brukerens modell og systemet, vil brukeren kunne gjøre feil eller feiltolke systemet.

Siden innloggingen er en del av systemet alle brukere skal gjennom, er det viktig at brukere er i stand til å forstå modellene som er involvert og logge seg inn. Passord representerer en modell for innlogging, men andre mekanismer representerer totalt forskjellige modeller, både i utforming og funksjon. Hvis de alternative mekanismene skal kunne benyttes er det viktig at brukere vil være i stand til å forstå dem, og danne seg korrekte mentale bilder av hvordan de fungerer.

I brukertesten er det mulig å studere hvordan brukere reagerer på de forskjellige mekanismene, hvordan de oppfatter og bruker dem. Hvis feil oppstår underveis, i hvor stor grad er brukerne i stand til å løse dem selv? Er det områder eller aspekter ved de ulike mekanismene som er vanskeligere å forstå og brukerne har problemer med? Hvilke teknikker kan benyttes for å bedre kommunisere hvordan systemet er bygget opp og hvilke muligheter brukeren har?

Kombinert med observasjonene, ønsker jeg samtidig å få tilbakemelding fra brukerene i forhold til hvordan de likte de ulike mekanismene, hvordan de var å forstå og hvilke mekanismer de foretrakk. Hvilken forståelse har brukerene av de forskjellige mekanismene? Er det deler av mekanismene som er uklare eller forvirrende? For denne delen ser oppgaven nærmere hvordan de mentale modellene kan være med å hjelpe brukerne i interaksjon med og i forhold til hvordan de oppfatter mekanismene.

Som en del av de ulike elementene som påvirker innloggingsprosessen, tenkte jeg det også var relevant å ta med deler av trusselbildet. Derfor er det interessant å spørre brukerne hva de ser som mulig trusler mot de forskjellige mekanismene og hvordan de vurderer sikkerheten på de enkelte. Både sett i forhold til hvordan de vurdere mekanismene i forhold til hverandre, men også hver for seg kan si en del om hvilke de anser som sikre og hvorfor. Trusselbildet utgjør en del av modellen brukere har for systemet, og hvilke trusler de anser som sannsynlige vil legge føringer på hvilke sikkerhetstiltak de benytter seg av for å redusere disse truslene. Ved å vurdere de ulike risikoene og hvor hensiktsmessig det er å bruke tid og krefter på å beskytte seg mot dem.

1.4 Oversikt over oppgaven

Resten av oppgaven er organisert som følger: neste del tar for seg teorien som ligger til grunn for oppgaven og historisk bakgrunn.

Del tre presenterer metodene som har blitt benyttet under arbeidet med oppgaven og diskuterer valg av metode.

Del fire beskriver selve caset og forskningsprosjektet rundt. Prototypen som blir benyttet i brukertesten blir beskrevet i detalj samt de forskjellige mekanismene som testes.

Resultatene og funnene fra observasjonene av brukertestene blir skildret i del fem. Denne delen dekker de ulike autentiseringsmekanismene samt en evaluering til slutt.

Del seks inneholder en diskusjon sett både i forhold til litteraturen innenfor feltet, men også hvilke funn som kom frem under brukertestene. Oppgaven avsluttes med konklusjoner basert på diskusjonen og tanker for videre forskning.

2 Teori

I denne delen vil jeg hovedsaklig legge frem bakgrunnen for oppgaven, både konkrete mekanismer for autentisering, og prinsipper innenfor HCI. Teorien vil ta for seg tre deler; hvordan autentiseringsmekanismer deles inn med eksempler, historisk bakgrunn, og til slutt konsepter og teknikker fra design av systemer med fokus på interaksjon mellom mennesker og maskiner.

2.1 Begreper

Siden oppgaven befinner seg i snittet mellom sikkerhet og menneske-maskin interaksjon (HCI), vil begreper og konsepter fra begge fagfelter benyttes.

Prosessen som foregår når en bruker logger seg inn, kan deles inn i tre. Først identifiserer brukeren seg for systemet, deretter autentiserer brukeren seg ved hjelp av en egnet mekanisme og ved vellykket autentisering blir brukeren autorisert av systemet. I en hensiktsmessig diskusjon om de forskjellige aspektene er det viktig å kunne skille mellom disse tre konseptene. Oppgaven fokuserer hovedsaklig på autentiseringen og mindre på de to andre aspektene.

2.1.1 Identifisering

Identifisering foregår ved at en bruker oppgir hvem personen utgir seg for å være. Det kan foregå enten enkeltstående eller som et ledd i en prosess, brukeren benytter seg av en mekanisme for å oppgi hvem personen er. På grunnlag av identiteten kan systemet så avgjøre om den oppgitte personen er en registrert bruker eller ikke. For et nettsted er identiteten ofte brukernavn eller e-postadresse. Et vanlig bilde på identifisering er å oppgi navnet sitt eller vise legitimasjon.

2.1.2 Autentisering

En definisjon av autentisering er "prosessen for å avgjøre identiteten til en kommuniserende part eller opphavet til en melding" [38]. En annen er autentisering definert som valideringen av en bruker eller prosess som bekrefter at de faktisk er den de utgir seg for å være [8]. Daler et al [5] definerer autentisering som fremlegging av bevis for at noen er den de utgir seg for å være. I forbindelse med identifisering er autentiseringen den prosessen brukeren går gjennom for å bekrefte at han eller hun virkelig er den oppgitte identiteten. Den typisk fremgangsmåten i en innloggingssituasjon er at brukeren først presentere hvem personen er via et brukernavn (identifisering) og deretter

bekrefter at brukeren er denne personen gjennom autentiseringen. Autentiseringen foregår i praksis ved hjelp av ulike mekanismer, f.eks. brukeren oppgir et passord.

Grunnen til å skille mellom identifisering og autentisering, er at flere kan gi seg ut for å være samme bruker, men ideelt sett vil uvedkommende ikke kunne bevise at de er brukeren. De blir dermed nektet adgang, mens rettmessige brukere kan bevise de er den de påstår og får tilgang, siden de vil selvfølgelig kunne bevise sin identitet.

Autentisering deles inn i tre hovedkategorier; basert på noe brukeren vet, noe brukeren har eller noe brukeren er [8] [24]. Målet for alle tre er å kunne benytte noe den legitime brukeren vet eller har, men som uvedkommende ikke vil ha tilgang til eller mulighet til å bruke. Forskjellige autentiseringsmekanismer baserer seg på en av disse tre kategoriene, men det er også mulig å kombinere mekanismer fra forskjellige kategorier. De forskjellige kategoriene og eksempler på mekanismer blir gjennomgått senere.

2.1.3 Autorisering

Autorisering er rettighetene som er gitt til en bruker eller prosess for å få tilgang til en ressurs [8], eller å få lov til å få tilgang til en ressurs [38]. Etter at brukeren har autentisert seg, vil autoriseringsprosessen sørge for å tildele de nødvendige rettigheter til brukeren. Som et ledd av innloggingsprosessen blir det vurdert hvem brukeren er og hvilke rettigheter personen skal ha. Et praktisk eksempel på autorisering er at en administratorbruker vil ha flere valg og muligheter tilgjengelig enn det en vanlig bruker vil ha mulighet til. Et annet ord for autorisering er tilgangskontroll, siden autoriseringen kontrollere hvem som har tilgang til ulike områder eller funksjoner i systemet. I hovedsak blir to metoder brukt for å håndtere autorisering; rollebasert og listebasert tilgangskontroll.

Ved rollebasert tilgangskontroll får en bruker tilgang til ressurser i basert på hvordan rollen assosiert med brukerens identifikasjon stemmer overens med rollen(e) som er autorisert til å få tilgang til innholdet [8]. Hver bruker kan ha forskjellige roller samtidig som gir tilgang til forskjellige ressurser. Sagt på en annen måte, basert på hvem og hva slags type brukeren er, blir det angitt hvilke deler av systemet brukeren har tilgang til. F.eks. vil vanlige brukere kun ha tilgang til fellessystemer, brukere tilknyttet økonomiavdelingen vil ha tilgang til regnskapet, administratorer vil ha tilgang over alt og så videre.

Hvis rollebasert tilgangskontroll benyttes, mener Daler et al [5] at autorisasjonen ikke bør være for finmasket, ellers blir administrasjonen omfattende. Hvis et større antall roller benyttes med overlappende eller ulike rettigheter,

blir det vanskeligere å avgjøre hvilke roller som har hvilke rettigheter, og hvilke rolle(r) en ny bruker skal tildeles. Det er derfor viktig å begrense antall roller til et oversiktlig antall, men det er likevel hensiktsmessig å dele inn brukerene i forskjellige roller slik at ikke alle brukere har full adgang til systemet. Derfor bør en avveining foretas for å sikre et nødvendig, men likevel oversiktlig, antall roller å dele inn brukerene etter. Med et større antall roller vil organisasjonen kunne miste oversikten over hvilke rettigheter de forskjellige rollene har, og hvilke som egner seg i et gitt scenario. Noen av ulempene med å miste oversikten er at det vil kunne oppstå redundante roller som håndterer de samme rettighetene, eller det oppstår sikkerhetshull ved at brukere blir tilknyttet andre roller enn de skulle og får flere rettigheter enn tiltenkt. Daler et al [5] peker også på at rollene bør revurderes etter hvert som tiden går og ressurser endrer status, i tilfelle høyere sikkerhetsklarering kreves for ressurser eller andre endringer er nødvendig.

Den andre metoden er listebasert tilgangskontroll, som vil si at brukere får tilgang hvis identifikasjonen oppgitt finnes på en liste over brukere som er assosiert med ressursen som etterspørres [8]. Istedenfor at brukerne blir tildelt ulike roller, blir de altså knyttet direkte opp til de ulike ressursene. Systemet vil så kontrollere om brukeren har tilgang til en bestemt ressurs når brukeren etterspør ressursen.

Listebasert tilgangskontroll har også noen av de samme utfordringene som rollebasert. Det kan bli lett å få en veldig finmasket inndeling når tilgang til de ulike ressursene må spesifiseres for hver enkelt bruker. Det kan også bli komplekst og vanskelig å holde styr på for administratorer hvilke brukere som skal ha tilgang hvor. Spesielt gjør dette seg gjeldende hvis ressurser blir lagt til eller endrer status, og vil kreve mer tid og krefter for å oppdatere listene.

2.1.4 Tilordning

Tilordning er prosessen når brukere utstyres med brukerkontoer og de rettigheter de trenger for å ha tilgang til et gitt system eller applikasjon [5]. Herunder inkluderes registreringen av brukerens identitet og selve opprettelsen av brukerkontoen. Tilordning kan enten gjennomføres av en administrator som oppretter en bruker for vedkommende som skal få tilgang, eller vedkommende selv går gjennom en registreringsprosess som leder til at brukeren blir tilordnet en brukerkonto.

Etter at informasjonen om den nye brukeren har blitt oppgitt vil systemet opprette og lagre brukeren og tildele de nødvendige rettigheter i forhold til tilgangskontrollen som blir benyttet. Tilordning er dermed en todelt prosess bestående av den delen som en bruker eller administrator foretar seg og den

som systemet foretar seg basert på inndataene. For denne oppgaven vil det i hovedsak fokuseres på brukerens del av registreringsprosessen.

2.1.5 Brukbarhet

Brukbarhet (usability) er definert som evnen et produkt har til å bli brukt på en effektiv og meningsfull måte av brukeren det er beregnet på [8]. Begrepet brukervennlighet har blitt benyttet tidligere på norsk, men det kan være misvisende siden det sjelden er systemer som har blitt designet for å være "brukerfiendtlige". Derfor blir brukbarhet benyttet i denne oppgaven, siden det er mer dekkende. Brukeropplevelse er en fellesbetegnelse for alle deler av en brukers interaksjon med et datasystem, program eller nettside. Brukbarhet er et viktig element av hvordan et system er designet, og sier noe om hvor enkelt det er å ta i bruk og forstå hvordan systemet kan brukes. Hvis systemet ikke legger opp til bruk, eller er tvetydig blir det vanskeligere for brukere å ta systemet i bruk.

2.1.6 Kryptografi

Kryptografi er en felles betegnelse for prinsipper og metoder for å gjøre informasjon i klartekst uleselig for andre, og for å kunne gjenopprette den opprinnelige informasjonen til forståelig form [38]. Daler et al [5] definerer kryptering som en metode for å skjule innholdet av en skriftlig melding for uvedkommende. For å sikre at en melding kun kan leses av den rettmessige mottakeren, kan avsender kryptere den før den blir sendt. Mottakeren må da dekryptere meldingen før den kan leses. Et vanlig bilde er at senderen låser meldingen med en nøkkel, og mottakeren må ha en tilsvarende nøkkel for å kunne låse den opp igjen. Kryptografi danner grunnlaget som en av de underliggende sikkerhetsmekanismene for en rekke ulike systemer. Det er primært to metoders som benyttes i dag; symmetrisk og asymmetrisk kryptering.

Ved symmetrisk kryptering blir den samme nøkkelen benyttet av både sender og mottaker for å kryptere og dekryptere meldingen. Sender og mottaker må dermed på forhånd blitt enige om hvilken nøkkel som skal benyttes før meldingen sendes. Daler et al [5] peker på at denne fremgangsmåten kan være problematisk siden det krever at krypteringsnøkkelen på et tidspunkt blir distribuert til alle som er involvert i transaksjonen. De foreslår at to parter helst bør benytte en ny felles nøkkel når de kommuniserer for å være trygge på at informasjonen er utilgjengelig for uvedkommende. Et alternativ vil være å benytte en asymmetrisk krypteringsmetode, der et er enklere å håndtere og distribuere nøkler.

Ved bruk av asymmetrisk kryptering blir det brukt to ulike nøkler, en

hemmelig og en offentlig. Den hemmelige nøkkelen er kun kjent for den som eier den, mens den offentlige er allment kjent. Denne metoden er også kjent som "offentlig nøkkel"-kryptering, siden den ene nøkkelen blir publisert mens den andre holdes privat. En viktig forutsetning for en god asymmetrisk kryptering er at kunnskap om den ene nøkkelen ikke gir noen kunnskap om den andre i paret [29]. Dermed kan avsender kryptere meldingen med mottakers offentlige nøkkel, siden kun den som har den private nøkkelen vil kunne låse opp meldingen. Avsender kan dermed vite at kun den rettmessige mottakeren skal kunne låse opp meldingen. Krypteringsnøklene gjør det også mulig for avsender å signere meldingen slik at mottaker vil kunne vite at bare den personen som hadde tilgang til den private nøkkelen kan ha sendt meldingen.

Et problem som symmetrisk kryptering ikke løser er utvekslingen av nøklene som er nødt til å foregå på et tidspunkt. For at begge sider skal kunne lese beskjeden må de ha tilgang til nøkkelen, men samtidig vil de hindre at uvedkommende får tak i nøkkelen slik at de ikke kan lese meldingen. Preneel [41] argumenterer med at krypteringen ikke løser problemet med å utveksle en hemmelig melding mellom to parter, men heller reduserer problemet fra en lengre melding til en kort nøkkel. Nøkkelen kan utveksles mellom partene på forhånd. Asymmetrisk kryptering løser derimot dette problemet, siden partene står fritt til utveksle den offentlige nøkkelen, mens de beholder den private for seg selv.

2.2 Datasikkerhet

Daler et al [5] definerer datasikkerhet som "beskyttelse mot brudd på konfidensialitet, integritet og tilgjengelighet for den informasjonen som behandles av systemet og systemet i seg selv". Konfidensialitet i denne sammenheng er å sikre at kun autoriserte personer får tilgang til informasjon på bakgrunn av at det tidligere har blitt foretatt en gyldig identifisering og autentisering av personen. For å opprettholde datasikkerheten, er autentiseringsmekanismene et av de kritiske elementene. Mekanismer som uvedkommende lett kan forbigå, eller få tak i brukeres informasjon vil sette datasikkerheten i fare. Ulike trusler og angrepsmetoder finnes, men for de fleste er det mulig å forsvare seg.

2.2.1 Sikkerhet i flere lag

Et viktig aspekt av sikkerhet er at en løsning vil kun være like sterk som det svakeste ledd. Hvis enkelte deler peker seg ut som mindre sikkert enn de andre delene vil angripere kunne fokusere på disse delene. Wing [50] organiserer løsninger i en opp-ned pyramide, der kryptografi ligger i bunn, over kommer

protokoller, så system og programmeringsspråk og på toppen applikasjoner. For at hvert ledd i pyramiden skal være sikkert kan det ikke være noen feil i de underliggende nivåene. Det hjelper lite om implementasjonen er korrekt hvis spesifikasjonen for protokollen inneholder feil [50]. Det er også mulig å se at lengre opp i pyramiden vil utviklere og designere ha mindre kontroll over omgivelsene og de forutsetningene som ligger til grunn. De valg som har blitt tatt i nivåene under legger retningslinjer for hvilke løsninger som er mulige. Også Muhammad et al [27] er enig i at designere og utviklere er sterkt avhengige av de underliggende protokollene for å kunne lage et sikkert system. Spesielt er det underliggende systemet for kryptering et av de kritiske elementene for autentiseringsprotokoller.

For å best kunne ivareta sikkerheten er det viktig at nye løsninger faktisk forbedrer sikkerheten og at eventuelle sikkerhetshull eller sårbarheter i nye forslag blir adressert før de tas i bruk. I løpet av utvikling av nye løsninger har flere protokoller blitt forkastet pga svakheter og feil i designet. Et mulig problem, som Torres et al [47] trekker frem, er mangelen på gode kriterier for å utvikle protokoller. Uten klare retningslinjer for hvordan sikkerhetsprotokoller utvikles for å sikre en trygg og sikker løsningen, blir det naturlig at enkelte løsninger kommer til kort allerede i designfasen.

For å kontrollere protokollene for feil, eller finne sikkerhetshull, blir de gjennomgått av forskere og andre eksperter, men ulike verktøy kan også benyttes. Å kunne garantere at sikkerhetsprotokollene fungerer som de skal er viktig innenfor flere felt. Wing [50] ønsker mer bruk av formelle modeller i utviklingen av nye metoder for autentisering og at de verktøyene som finnes blir bedre inkludert i utviklingsprosessen enn det de er per i dag. I tillegg til å føre formelle bevis, finnes flere verktøy for automatisk testing av protokoller som ser etter tilstander som oppstår når protokollene benyttes for å oppdage feil eller mangler. Det er så mulig å gå gjennom de forskjellige tilstandene for å se om det er noen veier som matcher et vellykket angrep. Ved å kunne avdekke problemer og feil tidligst mulig, vil det være mulig å rette dem før løsninger tar i bruk den eksisterende versjonen og bygger videre på et usikkert fundament.

Muhammad et al [27] legger vekt på policyer, mekanismer og kontrollering som de tre viktigste delene for å sikre system. Ved å etablere en klar policy for hvordan oppgaver skal utføres, blir det samtidig angitt hvilke retningslinjer som skal gjelde og hvordan sikkerheten skal fungere. Policyene vil variere avhengig av oppgaven og også avhengig av kontekst, siden en policy som kan være nyttig i en sammenheng ikke nødvendigvis er det i andre. Mekanismene blir utviklet med utgangspunkt i policyene. De er ment som forskjellige måter for å oppnå sikkerhetsmål som policyene angir. For å sette fornuftige mål er det viktig med forståelse av de truslene som kan ramme

systemet og en risikovurdering av hvilke som er mest sannsynlige. Basert på en risikovurdering, utvikles de mekanismene som anses som mest effektive for å oppnå målene i forhold til de truslene systemet står ovenfor. Målene bør derfor være klart definerte når protokollen utarbeides, og kontrollerert at den oppfyller de målene den blir designet for [27]. Til slutt bør systemet kontrollere for å se om systemet er i henhold til policy, og opprette planer for hvordan det skal håndtere hvis et suksessfullt angrep oppdages.

2.2.2 Sårbarheter

Det er utallige trusler og sårbarheter som kan ramme et system. Det er ikke hensikten å dekke alle i detalj, siden det ville blitt for omfattende, men heller trekke frem et representativt utvalg som er aktuelle i forbindelse med innlogging.

Virus og malware blir brukt som fellesbetegnelser for ondsinnet programvare, og er en velkjent trussel mot datamaskiner. Noe av malwaren er i stand til å overvåke brukeren og registrere hva brukeren foretar seg, gjøre opptak eller logge hva som skrives på tastaturet (kjent som keylogger). Det er dermed mulig å oppdage brukerens brukernavn og passord til forskjellige tjenester og sende brukerens innloggingsinformasjon til uvedkommende. Denne oppgaven vil ikke drøfte hvordan virus og malware fungerer i detalj, men de er en generell trussel for de fleste autentiseringsmekanismer siden uvedkommende kan overvåke og registrere hva brukeren gjør.

Phishing og identitetstyveri er to andre farer. Datateknologi gir muligheter for å lure personer til å oppgi personlig informasjon ved hjelp av tilsynelatende pålitelig elektronisk informasjon [5]. Phishing blir brukt som en fellesbetegnelse for teknikker for å lure offeret til å gi fra seg personlig informasjon. Offeret blir typisk kontaktet gjennom e-post eller andre kommunikasjonskanaler og bedt om å oppgi brukernavn og passordet sitt. Meldingene har falsk avsender fra tjenester brukeren er medlem av og gir seg ut for å være legetime meldinger. Disse e-postene oppgir ofte en lenke som leder til en side som ligner på tjenesten brukeren benytter seg av, men som i virkeligheten er kontrollert av angriperene. Tall fra Daler et al [5] viser at per 2005, var det registrert 35 millioner phishing-angrep, og sannsynligvis er tallet langt høyere i dag. Ved å sende ut disse e-postene til en større mengder brukere, vil de kunne "fiske" brukernavn og passord fra ofre som går på. Angripere som får tilgang til denne informasjonen kan enten misbruke den selv eller selge den videre til andre. Grazioli og Jarvenpaa [13] hevder grunnene til at nettsvindel er såpass utbredt, er at Internett gjør det vanskeligere å identifisere gjenstander, individer eller organisasjoner og vanskeligere å avgjøre om de er autentiske enn i tradisjonelle kontekster. Videre argumenterer de for at

kostnadene for å sette opp en troverdig side er forholdsvis lave, kombinert med at de kan nå ut til mange, og det er vanskeligere å straffeforfølge noen som har satt opp en webtjener i en annen del av verden.

I tilfeller hvor brukeren kommuniserer med en tjener over nettverket, kan kommunikasjonen være åpne for "mann-i-midten"-angrep. Her kan en angriper plassere seg mellom en klient og hovedtjeneren, og lure begge parter til å tro de kommuniserer med hverandre direkte. Angriperen vil dermed kunne se igjennom all informasjon før den blir videresendt og kan gi seg ut for å være andre for å få tilgang til tjenester. Hvis kryptering benyttes for mellom partene, blir det vanskeligere for angripere å gi seg ut for å være en av partene. Nettsteder som benytter kryptering er også utstyrt med sertifikater, som en mulig angriper må duplisere for å kunne gi seg ut for å være siden.

Et annet problem for nettverkstrafikken, er meldinger som sendes fra brukeren med informasjon som bekrefter hvem brukeren er. Hvis en angriper har tilgang til trafikken på nettverket, er det mulig å hente ut og lagre disse meldingene. Angriperen kan så sende de samme meldingene til tjenesten for å utgi seg for å være brukeren, i et såkalt gjenbruksangrep. Slike angrep vil derimot ikke fungere hvis meldingene som sendes kun kan benyttes en gang, eller de slutter å fungerer etter at brukerens sesjon er over. Så selv om angripere kan forsøke å gi seg ut for noen som allerede er logget inn, vil de bli nektet tilgang fordi brukeren har allerede benyttet seg av den meldingen selv.

Felles for de fleste mekanismer er at de alle er avhengige av å kontrollere informasjonen brukeren oppgir opp mot informasjon lagret i en brukerdatabase for å autentisere brukeren. Denne tjeneren vil være sårbar for tjenestenektangrep, også kjent som Denial of Service (DoS) eller Distributed Denial of Service (DDoS). Et tjenestenektangrep er en angrepsform der en eller flere brukere sender flere forespørsler til en tjeneste enn den klarer å håndtere. Siden tjeneren forsøker å håndtere den enorme mengden forespørsler, vil den bruke lengre tid på å svare hver enkelt eller i verste fall bli overbelastet og slå seg av. Formålet ved tjenestenekt er å stoppe eller delvis ødelegge en tjeneste hos en leverandør eller virksomhet [5]. Et godt bilde på tjenestenekt ville vært å samle en større gruppe mennesker for å ringe nødnummeret fra hver sin telefon. De som svarer får nok med å svare på unødvendige forespørsler, og legetime brukere blir nektet tilgang på grunnlag av den store mengden forespørsler.

2.2.3 Sikkerhet og brukere

Brukere blir generelt sett på som det svakeste leddet når det kommer til sikkerhet [46] [10]. Hvis applikasjonene eller den underliggende kryptografien

viser seg å motstå angrep, kan enkelte angripere sikte seg inn mot brukerene istedenfor. Ved hjelp av sosial manipulering (social engineering), eller utnytte kjente passord kan angripere omgå sikkerhetsmekanismene og få tilgang til systemet. Adams et al [1] hevder enkelte policyer for sikkerhet faktisk gjør systemene mindre sikre enn de kunne ha vært. I en undersøkelse fant de at en av hovedgrunnene til at folk valgte enkle passord eller skrev det ned, var fordi de var nødt til å bytte passord ofte, kanskje en gang i måneden.

Noe av årsaken er måten sikkerhet har blitt håndtert på. Brukere har blitt sett på som svakeste ledd og en del av systemet som ikke kan stoles på. Som en følge, er mye sikkerhet organisert rundt en "need-to-know"-filosofi, der brukeren kun får absolutt minimum av informasjon de trenger i forhold til sikkerhet. Adams et al [1] mener denne filosofien er skadelig, og gjør at brukere får mye av ansvaret for å opprettholde sikkerheten uten tilstrekkelig informasjon om hvordan et sikkert system er bygget opp. Siden brukerene ikke blir godt nok informert har de mindre kunnskap om de faktiske truslene og metodene og danner isteden sine egne modeller. Paradoksalt nok kan den manglende kunnskapen og tilbakemeldingene føre til at brukerene tar avgjørelser på feilaktig grunnlag. Uten tilbakemelding fra sikkerhetseksperter, visste brukere lite om hva som kjennetegnet et sikkert passord. De valgte passord basert på ord som finnes i ordbøker, eller navn.

Også Norman [33] ser på krav og policyer som et av punktene som gjør det vanskeligere for brukere som benytter forskjellige systemer. Hvis det blir innført standarder for hvordan passord skal være, er det viktig for brukerene å kunne se grunnene eller nytten i de nye reglene. Hvis ikke, vil de oppfatte dem som en komplisering og vanskeliggjøring av de arbeidsoppgavene de forsøker å utføre. Norman [33] går så langt som å hevde at hvis et system blir gjort sikrere, blir det i virkeligheten mindre sikkert siden brukere vil finne snarveier eller metoder for å komme seg rundt. En underliggende årsak er manglede forståelse for de konseptuelle modellene rundt sikkerhet. Norman hevder designet er en viktig del av å lage en løsning brukere aksepterer. Han trekker frem en dørlås som et eksempel, som gjør det vanskeligere å komme inn eller ut av et hus, samt at det krever mer tid. Likevel godtar vi låsene siden de har en klar nytteverdi, nemlig å kunne hindre andre adgang til huset. På bakgrunn av nytteverdien, ansees bruk av dørlåser som en forholdsvis grei bruk av tid og krefter.

Norman foreslår at vi trenger bedre metoder for å utforme systemer som passer bedre for brukerene. Systemene trenger en klar konseptuell modell og bedre tilbakemelding, for at brukerene skal bedre kunne forstå kravene rundt bruken av systemene. Norman konkluderer med at hvis brukerene bedre forstod grunnene, ville de være mer innstilt på å betale prisen for ekstra sikkerhet, på samme måten som de godtar å låse huset sitt med en nøkkel.

2.3 Autentiseringsmekanismer

Etter hvert som nye systemer har blitt utviklet og trusselbildet har endret seg, har nye mekanismer for autentisering blitt utviklet. Ulike mekanismer har som mål å forbedre sikkerheten eller fungere som alternativer til tradisjonelle mekanismer, enten for mindre brukergrupper eller for alle. Som nevnt tidligere, deles autentisering inn i tre kategorier; noe brukeren vet, noe brukeren har, eller noe brukeren er. Ulike autentiseringsmekanismer tilhører en av kategoriene. I hver av kategoriene har ulike mekanismer blitt foreslått, og prøvd ut i forskjellig grad.

2.3.1 Noe brukeren vet

Noe brukeren vet tar utgangspunkt i at brukeren skal vite eller rettere sagt huske noe som gjør at personen kan få tilgang. Brukeren skal holde hva personen vet skjult fra andre, og oppgi det under autentiseringen for å bevise at det er den rettmessige brukeren. Dette dekker passord, passfraser, bildekombinasjoner eller andre elementer brukeren skal huske.

Passord eller passfraser

Passord er sannsynligvis den meste kjente og mest brukte mekanismen for autentisering, og vil derfor ikke bli gjennomgått i detalj. Den fungerer ved at brukeren husker en kombinasjon av ord eller tegn som brukeren oppgir ved innlogging.

Mye av styrken i passord kommer av tegnkombinasjonen brukeren har valgt seg og hvor vanskelig den er å gjette for andre. Kjente teknikker for å finne ut andres passord er å gjette seg frem, prøve lister med ord som ofte blir brukt som passord, automatiske angrep med ordlister som inneholder en rekke ord inkludert med mindre feilstavinger. I verste fall kan en angripere forsøke å gjette seg frem ved å forsøke alle muligheter (kjent som brute force). For angripere der målet er å få tilgang til brukeres informasjon kan disse enkle angrepene være nok til å "knekke" de enkleste passordene.

Grafiske passord

Det har vært flere forslag til hvordan grafiske passord kan benyttes istedenfor passord basert på tekst. Suo et al [46] mener de fleste kan deles inn i en av to hovedkategorier; basert på noen brukeren skal huske eller kunne kjenne igjen. I mekanismer basert på gjenkjennelse blir brukeren presentert for et utvalg bilder der brukeren skal identifisere et bilde som ble valgt ut ved registrering. For mekanismer basert på å huske noe må brukeren reprodusere noe brukeren

valgte eller oppga ved registrering. Selv om det er den jevne oppfatningen at grafiske passord vil være enklere å huske enn tekst, er det lite bevis som støtter dette argumentet. Suo et al [46] viser til psykologistudier som slår fast at mennesker er bedre til å huske bilder enn tekst, og argumenterer for at det er sannsynlig at det vil kunne gjøre grafiske passord enklere å huske. I en annen studie ble det vist at brukere i større grad var i stand til å logge inn ved å huske bilder kontra å huske et passord. Samtidig la de merke til at tiden det tok å logge inn økte. Undersøkelsen Suo et al har utført tyder likevel på at grafiske passord er vanskeligere å knekke med tradisjonelle angrepsmetoder som brute force, ordbokangrep eller spionvare. På den annen side er ikke disse systemene særlig utbredte, så det er mulig vi ennå ikke har god nok oversikt over sårbarhetene grafiske passord står ovenfor. Suo et al [46] har sett på en rekke forskjellige forslag til grafiske passord, og vi vil ta for oss noen av de som har blitt diskutert.

For mekanismer som tar utgangspunkt i passord basert på bilder, er det et par trekk som går igjen. Brukeren velger seg et visst antall bilder ved registrering, og skal senere oppgi et eller flere av dem for å autentisere seg. Siden det kan bli for enkelt for uvedkommende å plukke ut et bilde fra et utvalg for å logge seg inn, har det blitt foreslått å ta innloggingen i flere ledd, som fører til at brukeren må plukke ut flere bilder. Ulempen med denne fremgangsmåten er at innloggingen tar lengre tid.

Det har blitt fremmet ulike forslag for mekanismer basert på gjenkjenning som tar utgangspunkt i å tegne opp eller gjenta et utvalg. En mekanisme hvor det har vært ulike forslag er ved å tegne et mønster eller figur i et rutenett. Brukeren kan selv velge hvordan figuren skal se ut, og om den innholder punkter, streker eller en kombinasjon. Gitt en viss lengde på figuren som skal tegnes og størrelsen på rutenettet, kan det være vanskeligere å gjennomføre et ordbokangrep mot grafiske passord. Hvis figuren er avansert nok vil mulighetene bli for mange til at alle mulige mønstre lett kan dekkes av en ordbok. Et mulig problem er at mennesker har lettere for å huske symmetriske figurer enn usymmetriske, og det kan derfor tenkes at mange vil bruke symmetriske figurer. Siden mulighetene for symmetriske figurer mindre enn asymmetriske figurer, kan det gjøre at grafiske passord blir enklere å finne ut enn tekstbaserte passord.

En mulig løsning for å bøte på problemet kan være å øke lengden på figuren som blir benyttet, som gjør at det likevel blir store muligheter og vanskeligere å gjette seg frem til brukerens mønster. Et annet lovende forslag er å tilby et større rutenett, der brukeren først velger ut et mindre område av rutenettet til å tegne selve figuren på. Som en tenkt situasjon kan det store rutenettet ha 100 ganger 100 ruter, der brukeren kan fritt velge et kvadrat på 20 ganger 20 ruter for å plassere sitt mønster. Dette øker mulighetene for

hvor mønsteret kan plasseres, og en angriper vil måtte først finne ut hvilket område av rutenettet brukeren tegner på og så finne ut av mønsteret.

Et åpenbart problem med grafiske passord er at når de vises på skjermen vil de være synlige for andre enn kun brukeren. Et mulig forslag for å gjøre det vanskeligere for andre å se hva brukeren velger er å plassere en større geometrisk figur rundt flere bilder, der kun et av dem var det riktige. Brukeren valgte med andre ord en gruppe bilder istedenfor et enkeltbilde. Hvis noen ser over skulderen til brukeren vil de dermed ikke kunne vite hvem av bildene som var det riktige. Et annet problem er hvis brukeren har valgt forutsigbare bilder. Spesielt i tilfeller der angriperen kjenner brukeren vil det være mulig å avgjøre hvilke bilder som er lagt til av brukeren.

Noen forsøk har basert seg på at brukere klikker på forskjellige steder i et bilde i en bestemt rekkefølge for å kunne logge seg inn. Bildene vil bestå av mange forskjellige punkter av interesse, og en bruker vil under registrering merke sine punkter i en bestemt rekkefølge. Hvert område vil ha et visst slingringsmonn slik at det ikke er nødvendig å trykke på det eksakt samme stedet markøren var på opprinnelig. En mulig sårbarhet er at bildene har naturlige områder som peker seg ut i bildene som brukerene velger, og angripere vil kunne gjette seg til. I tillegg får brukere en rekkefølge å huske på, der antall punkter kan variere utifra hva brukeren selv har valgt. I en studie der denne mekanismen ble sammenlignet med passord, trengte brukere færre forsøk med grafiske passord, men de hadde vanskeligere for å lære passordet kombinert med at innlogging tok lengre tid.

Selv om grafiske passord ikke er særlig utbredt, kan de gi fordeler i forhold til kjente angrepsmetoder for tradisjonelle passord. Det kan være vanskeligere gå gjennom alle muligheter for grafiske passord, og mekanismer med et større antall muligheter å velge fra vil ytterligere gjøre det vanskeligere. En fare som fortsatt er gjeldende er at angripere som kjenner brukeren godt kan gjette seg frem til hva personen ville ha valgt. Enkelte metoder for sosial manipulering vil derimot bli vanskeligere, siden det vanskelig å oppgi et grafisk passord over telefon.

Med mulighetene touch-skjermer gir, har Gao et al [10] foreslått at istedenfor å klikke direkte på bildene, kan brukere tegne linjer mellom dem. Spesielt vil slike mekanismer være tilpasset smarttelefoner eller andre touch-skjermer. Linjene blir ikke vist på skjermen, slik at brukeren kan streke mellom forskjellige bilder uten at andre vil kunne se over skulderen hvilke som blir valgt. En annen mulighet som gjør det vanskeligere for å andre å se over skulderen er å skulle trekke en linje gjennom en rekke bilder inkludert bilder som kanskje ikke er til å logge inn. I utvalget når brukeren skal logge seg inn, er det et startbilde og et stoppbilde. Brukeren skal trekke en linje fra det ene til det andre bildet innom brukerens valgte bilder, men kan også inkludere

andre bilder underveis. For hver gang brukeren skal logge seg inn blir bildene organisert i tilfeldig rekkefølge, slik at linjen mellom bildene endrer seg. For andre som ser over skulderen vil de ha vanskeligheter med å skille mellom hvilke bilder som skal med og ikke. For å unngå at brukeren oppgir start og slutt-bilde, velger systemet to tilfeldige bilder som start og slutt selv. Under brukertester fant Gao et al [10] to problemer med denne metoden. For det første valgte mange å starte å tegne linjen fra det første bildet i passordet sitt, ikke det bildet som ble tilfeldig valgt som utgangspunkt. Selv om det avtok etter hvert som brukerene hadde logget inn et par ganger, kan det likevel avsløre enkelte av brukerens bilder. I tillegg merket de at brukerene hadde en tendens til å ta pauser når de hadde kommet til et av de riktige bildene, før de gikk videre. Antageligvis trakk brukerene linjen til et av sine bilder, og stoppet så opp mens de lette etter neste. Disse pausene kan gjøre det mulig å se hvilke bilder som brukeren benytter for å logge seg inn.

2.3.2 Noe brukeren har

Noe brukeren har beskriver en gjenstand som brukeren har. Det er ofte mulig å ta med seg gjenstandene, og ha den med til stedet der brukeren ønsker å autentisere seg. Eksempler på noe brukeren har inkluderer smartkort, bankkort, kodegeneratorer eller nøkler. Et typisk eksempel er et adgangskort brukeren må ha med seg for å komme seg inn et sted, eller kodegeneratorer som kalkulerer et nytt passord hver gang brukeren skal logge seg inn. I det siste tilfellet slipper brukeren å huske på selve passordet, det holder å ha med seg kodegeneratoren som kan gi brukeren et nytt passord når det er behov for det.

Kort eller andre gjenstander brukeren har brukes ofte i kombinasjoner med andre mekanismer, som PIN-koder. Det er likevel mulig for tjenester å gi tilgang til brukere som autentiserer seg basert på noe de har.

2.3.3 Noe brukeren er

Til slutt har vi noe brukeren er, som dekker biometriske løsninger. Biometri er definert som analysen og kvantifiseringen av menneskelige karakteristikker til et digitalt format [8]. Det er mulig å dele denne kategorien ved å skille mellom noe brukeren er og noe brukeren gjør [24], men vi vil i denne oppgaven forholdes oss til begge deler i felleskap. Disse mekanismene tar utgangspunkt i at hver bruker er unik, som gjør at fysiske egenskaper eller bevegelser vil kunne knyttes til en person. Utgangspunktet er at er at uvedkommende ikke vil kunne replikere egenskapene eller bevegelsene og gi seg ut for å være en rettmessig bruker. Det finnes forskjellige mekanismer basert på

biometri, men felles for dem er at de alle omfatter teknologi som kan lese av menneskelige kjennetegn som fingeravtrykk, øye (iris), stemme, ansikt eller håndgeometri [5]. Det avleste mønsteret blir så sammenlignet med et allerede lagret mønster og det er på dette grunnlaget bruken blir nektet eller får tilgang. Dette forutsetter naturligvis at brukeren på forhånd har registrert seg og det har blitt lagret en signatur som tilhører brukeren.

Fordelen med biometriske mekanismer er at til forskjell fra noe brukeren vet er det ikke mulig å glemme. I forhold til gjenstander som brukeren har, er det heller (stort sett) ikke et noe brukeren mister eller ikke har med. De kan heller ikke deles med andre og blir også sett på som vanskelige å forfalske, som gjør at en del ser på biometriske mekanismer som lovende [17].

Et av problemene med biometri er at systemet for autentisering kan være kostbart, og prosessene kan være upålitelige [46]. Upålitelige prosesser kan slå begge veier, både ved at uvedkommende kan få tilgang, men også at rettmessige brukere sperres ute hvis de ikke kan benytte andre innloggingsmekanismer (f.eks. hvis gips dekker fingeravtrykk, eller brukeren har blitt forkjølet i forhold til stemmegjenkjenning). Et annet, større problem er at løsningen kan sette brukere i fare hvis uvedkommende vil ha tak i f.eks. en finger for å kunne logge seg inn med brukerens fingeravtrykk. Biometriske løsningner har derfor for det meste blitt benyttet til ikke-kritiske tjenester eller i kombinasjoner der det kreves en annen form for autentisering i tillegg.

Håndskrift

Historisk sett har underskrift og signaturer blitt brukt lenge før digital autentisering for å bekrefte at det er den rettmessige personen som undertegner noe. Som enkelte andre biometriske mekanismer tar signaturgjenkjenning utgangspunkt i en bestemt oppgave som brukeren utfører. Det er en mekanisme de fleste ville kunne benytte seg av, brukeren slipper å huske noe, og tiden brukt på innlogging ville ikke vært nevneverdig lang. Ifølge Radhika et al [42] er desverre metoder for å kunne verifisere håndskrift nøyaktig fortsatt et uløst problem.

Ved registrering skriver brukeren noe slik at systemet har en fasit for hvordan brukerens underskrift ser ut. Ved innlogging, oppgir så brukeren det samme på nytt, og det blir sammenlignet hvor likt det er med det opprinnelige bildet. Daler et al [5] ser likevel på underskrift som en god metode hvis både bevegelse og trykk blir registrert.

Skanning

Det er forskjellige elementer av kroppen som bli ansett som unike, noe som gjør at f.eks. fingeravtrykk eller iris vil knyttes til kun en person. De fleste mekanismene går ut på å skanne deler av kroppen, som så blir sammenlignet med en ny skanning hver gang noen forsøker å logge seg inn. Hvis brukeren som forsøker å logge seg inn allerede er registrert, får personen tilgang. Faren er at flere av skannerene har forbedringspotensiale og kan være unøyaktige ved hvem de tillater og ikke. Et annet problem for brukerene er hvis informasjonen som ligger lagret kommer på avveie. Passord eller andre elementer kan lett byttes ut, men fingeravtrykk er ikke lett å skifte for brukere hvis uvedkommende får tak i det og misbruker det.

Det er også skannere som observerer bevegelser, som gangelag. Dette er også egenskaper som blir sett på som unike og vanskelige å duplisere for andre. Mange av disse mekanismene er fortsatt under utvikling, men de kan likevel tas i bruk i flere sammenhenger. F.eks. nevner Jain et al [17] at skanning av håndflaten har allerede fungert bra som en mekanisme for å gi tilgang til bygninger eller rom.

2.3.4 Kombinasjon av kategorier

De ulike kategoriene har hver sine styrker og svakheter. F.eks. kan passord bli gjettet eller avsløret, adgangskort kan bli mistet eller stjålet osv. Siden hver kategori har ulike svakheter, argumenterer Daler et al [5] for at det autentiseringen blir sikrere ved å kombinere fra mer enn en kategori. Sikkerheten økes siden uvedkommende må overkomme flere mekanismer for å oppnå tilgang. Dette kalles flerfaktor autentisering, siden autentiseringen benytter seg av flere faktorer, eller kategorier. Et eksempel er minibank som krever en kombinasjon av bankkort (noe brukeren har) og PIN-kode (noe brukeren vet) for å gi tilgang til en konto. Avhengig av kombinasjonen vil to eller tre former for autentisering gi bedre styrke [8]. Valget av mekanismene vil selvfølgelig spille inn her, samt systemet de skal beskytte, men generelt sett vil mer enn en faktor øke sikkerheten.

I eksemplet med minibanken over, må uvedkommende både få tak i kortet til offeret, samt finne ut PIN-koden for et suksessfylt angrep. Kombinasjonen er vanskeligere å angripe enn hver mekanismene hver for seg. Det gjør også at kort eller andre gjenstander som kommer på avveie blir et mindre problem, siden de ikke kan brukes alene. Gjenstander brukeren har brukes ofte som et element i flerfaktor autentisering, i kombinasjon med noe brukeren vet som med bankkort/PIN-kode ovenfor. Enkelte velger å ta utgangspunkt i passord, og utvide denne mekanismen ved å legge til en annen faktor for å

gjøre løsningen tryggere.

2.3.5 Single sign-on

Single sign-on beskriver tjenester som gjør det mulig å logge på forskjellige steder med samme brukerinformasjon, f.eks. brukernavn og passord. SSO består av tre komponenter; hovedtjener, tjenester og klienter [52]. Dette fører til at SSO-tilbyderen kommer inn som en tredje part i innloggingsprosessen, i tillegg til brukeren og tjenesten som er vanlig. Istedenfor at tjenesten selv håndterer innloggingen og brukerinformasjonen, baserer de seg på at brukerene logger seg inn via SSO-tilbyderen. Tjenestene behandler denne tilbyderen som en betrodd tredjepart, der de sender brukere som ønsker å logge inn. Når brukerene har vellykket logget seg inn, blir de sendt tilbake igjen til den tjenesten de kom fra sammen med informasjon om at brukeren er innlogget. Hvis brukeren besøker andre tjenester som også benytter seg av SSO, vil brukeren enkelt kunne logge inn der også uten å oppgi brukerinformasjonen på nytt. Når tjenestene sender brukeren videre til innloggingen gjennom SSO, vil tilbyderen legge merke til at brukeren allerede har autentisert seg og sende brukeren tilbake til tjenesten. SSO fungerer mye på samme måte som når brukeren går til et annet sted innenfor en tjeneste eller et nettsted hvor brukeren allerede er logget inn, men forskjellen er at SSO spenner seg over ulike systemer.

Det er umiddelbart mulig å se en fordel med SSO sett fra brukerens synspunkt. SSO gjør at brukere slipper å holde styr på ulike brukernavn og passord for de forskjellige systemene de er medlem av hvis de alle er knyttet sammen. Dette gjør det mulig å redusere antall brukerkontoer i bytte mot en litt annerledes prosess under innloggingen. Fra brukerens synspunkt kan dette minne om en universal nøkkel, eller bankkort som kan brukes på ulike terminaler i forskjellige butikker som ikke er tilknyttet hverandre.

Med bruk av SSO kan antallet passord kan reduseres, siden flere tjenester kan benytte samme, felles passord. Det kan også tenkes det passordet kan gjøres mer komplisert og sikkert, siden brukeren kan fokuser på å huske det ene fremfor en rekke forskjellige. På den andre siden øker dette det potensielle skadeomfanget hvis uvedkommende får tilgang, siden de vil kunne ramme alle de forskjellige tjenestene passordet gir tilgang til. Analogien som ofte benyttes innenfor sikkerhet, er å ikke legge alle eggene i samme kurv. Tanken er at hvis noe går galt (mister kurven), går det utover alle tjenestene (eggene knuses). Det er derfor en god ide å ikke binde seg til kun en løsning, slik at en mulig angriper ikke får tilgang til alt.

2.4 Historisk bruk av autentisering

2.4.1 Tidlige datamaskiner

Helt fra datamaskiner ble introdusert har det vært et behov for å kunne skille ut legetime brukere som skal ha tilgang til systemene fra de som ikke skal ha det. Tidlige sikkerhetsstandarder ble utviklet av det amerikanske militæret, og fokuserte for det meste på den fysiske sikkerheten [51]. Det fantes få maskiner, og de få mainframene som var tilgjengelige kunne koste alt fra flere hundre tusen opp til millioner av dollar. Det første tiåret etter andre verdenskrig, bestod sikkerheten typisk av at området der datamaskinen ble oppbevart var sikret. Siden datamaskinen var såpass store, var de ofte plassert i egne rom som kunne sperres av, og kun legetime brukere fikk tilgang. Sikkerheten var i stor grad rettet mot trusler som tyveri eller vandalisme, og vakthold og alarmer ble benyttet for å hindre adgang fra uvedkommende.

2.4.2 Maskinene kobles sammen i nettverk

Etterhvert som mainframene ble mer utbredt og minimaskinene ble introdusert, ble det stadig vanskeligere å håndheve den strenge fysiske sikkerheten. Samtidig ble maskinene koblet sammen i nettverk utover 50- og 60-tallet. Dermed fikk vi nettverk der maskinene var koblet sammen over telefonnettet, og ulike brukere kunne logge seg på og dele på ressursene, gjennom timeshare. Brukere kunne koble seg opp fra terminaler til større maskiner. Hver terminal gjorde det mulig å logge seg inn, men hoveddelen av programmene ble kjørt og informasjonen ble lagret på eksterne maskiner terminalen var koblet opp til. Når det var sin tur, kunne brukerene kjøre programmer eller hente frem resultater fra forrige kjøring. Da nettverkene var blitt bygget hadde de forskjellige maskinene blitt koblet sammen som en del av et voksende, åpent system der nye maskiner kunne legges til.

Tidlig på 70-tallet ble det slått fast at det ikke var mulig å ha det nivået av sikkerhet som enkelte ønsket i åpne systemer. Stadig ble flere maskiner lagt til, og nye brukere fikk tilgang til både maskinene og nettverket. I utgangspunktet hadde alle brukere tilgang til all informasjon lagret på maskinene de logget seg inn på, som i visse tilfeller inkluderte informasjon de ikke burde ha tilgang til. En løsning for å bøte på problemet var å dele inn informasjonen som var lagret i forskjellige nivåer, slik at brukere ikke fikk tilgang til informasjon de ikke var klarerte til å behandle. Med andre ord ble brukerene fra nå av autorisert i forhold til de ressursene de skulle ha tilgang til.

2.4.3 Internett

Et av de viktigste teknologiske forutsetningene for at Internett kunne spre seg, var pakkesvitsjing som ble funnet opp på tidlig 60-tall. Pakkesvitsjing vil si at meldingene som blir sendt deles opp i mindre deler, kalt pakker, som så sendes over nettverket. Hver enkelt pakke kan ta ulike veier før de kommer frem dit de skal. Når de ankommer mottakeren, blir de satt sammen igjen til den opprinnelige meldingen. I 1965 fikk vi det første vidstrakte nettverket mellom en maskin i Massachusetts og en i California [23]. Dette viste at maskiner kunne jobbe sammen, også over store avstander, men telefonlinjene som ble brukt var upassende til formålet, og bekreftet nødvendigheten av pakkesvitsjing [23]. Basert på dette forsøket, gikk Defense Advanced Research Projects Agency (DARPA) inn for å videreutvikle nettverk, som ledet til ARPANET, som var det første større datanettverket. Første node i nettverket ble koblet til i 1969, og flere noder ble lagt til utover 70-tallet.

Tidlig på 1970-tallet utviklet Robert Khan og Vinton Cerf en protokoll som ble til Transmission Control Protocol/Internet Protocol (TCP/IP). Den baserte seg på at ARPANET (som Internett idag) skulle ha en åpen arkitektur hvor hvem som helst skulle kunne koble seg til. For nykommere som sluttet seg til nettverket skulle det ikke spille noen rolle hvilke teknologi eller leverandører de brukte, så lenge de kunne kommunisere med de andre maskinene.

TCP ble i utgangspunktet designet for å håndtere all transport og videresending. TCP baserte seg på pakkesvitsjing, og skulle sikre at alle pakkene som ble sendt også kom frem til mottaker. Dette inkluderte også å ta ansvaret for pakker som ankommer i feil rekkefølge, pakker som går tapt eller pakker som mottas flere ganger [5]. Hvis feil oppstod, ble de rettet ved å sende pakkene på nytt. Etter hvert viste det seg at i enkelte tilfeller burde ikke pakketapet bli rettet av TCP, men bli bedre håndert av applikasjonen [23]. Protokollen ble da splittet i to; TCP og IP. TCP skulle fortsatt ta for seg flytkontroll og håndtering av tapte pakker, mens IP skulle håndtere adresseringen og videresending av individuelle pakker. Det ble også utviklet en alternativ protokoll, User Datagram Protocol (UDP), som et alternativ til TCP som kunne brukes sammen med IP.

Tidlige implementasjoner av TCP ble skrevet til timeshare systemer, og da PCer ble introdusert, trodde en del at protokollen var for stor og kompleks til å kunne kjøre på disse [23]. Men det viste seg fort også PCer kunne være en del av Internett. Med utbredelsen av PCer og lokale nettverk utover 80-tallet, vokste Internett.

Internett ble i første omgang tatt i bruk av forskere, og Leiner et al [23] ser i ettertid at å inkludere Internett-protokollene i et operativsystem for

forskermiljøet var et viktig ledd i å spre Internett. Kombinert med muligheten til å foreslå og diskutere nye ideer til protokoller gjennom RFCer (request for comments), var det samtidig mulig å kunne bidra i diskusjonen og forme de standardene som ble tatt i bruk. Med muligheten til å ikke bare foreslå nye protokoller, men også dynamisk utvide og legge til nye tjenester, danner Internett en plattform med grobunn for et ukjent antall nye tjenester. Daler et al [5] argumenterer for at en av ulempene er at dette stiller større krav innen sikkerhetsplanlegging og oppfølgning.

TCP/IP sender i utgangspunktet all kommunikasjonen i klartekst over nettverket. På samme måte som endringer ble gjort på begynnelsen av 70-tallet for å hindre at brukere skulle ha tilgang til all informasjonen på maskinene i nettverket, har det blitt lagt til mekanismer for å beskytte datatrafikken. For å hindre at trafikken kan fanges opp eller leses av andre, kan informasjonen bli kryptert før den sendes, og dekryptert av mottaker for å sette sammen den opprinnelige meldingen. Når trafikken mellom klient og tjeneren er kryptert, vil ikke uvedkommende kunne tyde meldingene, selv om de er i stand til å fange dem opp. Klienten og tjeneren bestemmer seg samlet for hvilke krypteringsnøkler som skal benyttes til kommunikasjonen seg imellom [5]. En mulighet for kryptering av trafikken er Secure Socket Layer (SSL). SSL ble introdusert i 1994 og senere erstattet av Transport Layer Security (TLS). TLS og SSL er særlig brukt i forbindelse med webapplikasjoner og i nettlesere.

2.4.4 Grafiske brukergrensesnitt

Mens datamaskiner ble tatt mer i bruk, både i bedrifter og privatpersoner, endret metodene for bruk av maskinene seg. Myers [28] tar for seg utvikling på maskinsiden i menneske-maskin interaksjon siden datamaskinene ble introdusert. De fleste grensesnittene kommer fra forskningsmiljøer, før de senere har blitt adoptert av industrien. Et mønster som gjentar seg er at nye metoder blir benyttet i rent forskningsøyemed, før de blir forsket på også i industrien før de ender opp i kommersielle produkter. De fleste grensesnittene og mekanismene vi har i dag for interaksjon med datamaskiner er i stor grad basert på og viderutviklinger av tidligere grensesnitt. Det grafiske brukergrensesnittet i operativsystemer som tar utgangspunkt i vinduer, ikoner, menyer og pekere kan spores tilbake til tidlige versjoner av Macintosh som fikk ideene fra Xerox PARC, som igjen baserte seg på tidlig forskning fra Stanford Research Laboratory og Massachusetts Institute of Technology.

Tidlig i historien ble for det meste kommandolinjebaserte grensesnitt benyttet, der brukere kunne skrive inn ulike kommandoer som så ble kjørt av maskinen. Grensesnittet for direkte manipulering, der elementer på skjermen

kan manipuleres ved hjelp av pekeredskaper ble først demonstrert i 1963. I begynnelsen ble lyspenner benyttet for å manipulere elementer, men i 1965 utviklet Stanford Research Laboratory en erstatning for lyspenner: mus. Den ble mer kjent som en praktisk inndataenhet utover 1970-tallet takket være Xerox PARC. Sammen med den nye enheten for inndata, ble det også etter hvert større fokus på grafiske brukergrensesnitt fremfor kommandolinjen. Mus brukt i maskiner fra Xerox, og også tidlige Apple-maskiner på begynnelsen av 1980-tallet, inkludert Apple Lisa (1982) og Apple Macintosh (1984). Samtidig som pekeenhetene ble utviklet, så brukerene også forandring i utforming på skjerm. Ikoner var et begrep som først ble brukt av David Canfield Smith i sin doktoravhandling i 1975, og som ble tatt i større bruk utover 70-tallet. Ikonene gjorde det mulig å ha representasjoner av programmer og filer lagret på maskinen. På samme tid gjorde begrepet "WYSIWYG" (What you see is what you get) seg gjeldende, og bla. tekstbehandlere ble utviklet der teksten ble presentert slik den ville se ut i en endelig versjon, mens brukeren kunne skrive eller redigere den. Et annet nytt element var vinduer, en rekke forskjellige vindusbehandlere der vinduene kunne overlappe hverandre eller bli plassert ved siden av hverandre.

Samlet ga de nye grafiske elementene Vinduer, ikoner, menyer og pekere (av engelske Windows, icons, menus and pointers (WIMP)) et utgangspunkt for interaksjon med datamaskiner gjennom grafiske brukergrensesnitt. Myers [28] hevder disse elementene nå er inne i en standardiseringsfase, der de fleste benytter den samme teknologien med kun små, inkrementelle endringer. Derfor er det viktig å kunne se på og forske videre på nye metoder for brukerinteraksjon i fremtiden. Nye metoder for interaksjon vil også kunne åpne for nye metoder for brukerinnlogging og autentisering.

2.4.5 Hypertekst og World Wide Web

Verdensveven, eller World Wide Web, er en fellesbetegnelse for de ulike nettstedene som finnes og er tilgjengelig over Internett. Den åpne arkitekturen i Internett gjorde det mulig å legge til verdensveven, men mye av suksessen skyldes også hvordan forskjellige nettsteder kan knyttes sammen. Siden nettstedene inneholder hypertekst, er det er mulig å danne koblinger (lenker) fra en side til en annen, som brukere kan benytte seg av. Hypertekst tar utgangspunkt i ideer som ble presentert allerede i 1945, av Bush [3]. Bush var opptatt av hvordan kunnskap kunne gjøres mer tilgjengelig. Forutsatt at all verdens kunnskap var blitt lagret, ville det fortsatt være et stort problem å kunne foreta nyttige utvalg av informasjonen. Istedenfor å gjøre oppslag i data som var blitt lagret alfabetisk eller numerisk, foreslo Bush en alternativ måte å organisere informasjonen på. Ved å organisere gjenstander i et nett

(vev), ville det være mulig å koble sammen elementer som hørte sammen, på samme måte som vi benytter assosiasjoner når vi tenker. Dette ville gjøre det enklere å gå fra en tekst til annen relatert informasjon. Brukerene ville også kunne danne nye koblinger og danne stier mellom tekstene som danner et nettverk det vil være mulig å utforske og navigere seg langs.

Konseptene og prinsippene Bush presenterte minner mye om hvordan World Wide web i dag er organisert ved hjelp av hypertekst. Selv om konseptet er likt, ble begrepet hypertekst først brukt i 1965 [28]. Forskjellige systemer med støtte for lenker mellom dokumenter ble utviklet utover 1960 og 70-tallet. Disse ble i hovedsak brukt til å publisere vitenskapelige artikler der det var mulig å kunne lenke til artikler som ble sitert. I 1983 kom det første systemet hvor det var mulig å klikke på lenker for å gå til en annen side. Det har senere vært flere forskjellige hypertekstsystemer, men det mest kjente er World Wide Web, skapt av Tim Berners-Lee i 1990. Verdensveven danner et nettverk av utallige nettsteder som fritt kan lenke videre til andre, og som brukere kan utforske for å finne lignende materiale som de ønsker.

Firmaer og organisasjoner etablerte seg på verdensveven, som ledet til en eksplosjon i antall virus og angrep. Uvedkommende forsøkte å få tilgang til hva bedriftene hadde lagt ut, eller komme seg inn på de interne nettverkene. Som forsvar, svarte mange ved å sette opp brannmurer, som gjør det mulig å filtrere eller blokkere tilgang til ressurser. Brannmurene tok det noe naive utgangspunktet at brukere på det interne nettverket var godkjent til å få tilgang, mens brukere utenfra ble nektet tilgang [6]. Problemet med denne antagelsen oppstår når noen innenfor bestemmer seg for å utnytte den tilgangen de har, eller gi andre tilgang.

Sammen med firmaer og organisasjoner sitt inntog på verdensveven, ble utallige nettsteder etablert, dedikert til ulike interesseområder. Det var også mulig for vanlige brukere å lage sine egne sider. Siden da har større portaler, og sosiale nettsteder som Facebook, twitter og myspace etablert seg.

For at nettstedene skulle kunne håndtere og skille mellom forskjellige brukere, var det nødvendig med mekanismer for å logge inn på nettsteder. Siden kommunikasjon benyttet den tilstandsløse protokollen HTTP (Hypertext Transfer Protocol), var det vanskelig å kunne skille mellom de forskjellige besøkende hos en side. Når brukeren etterspurte en ny side ble forespørselen håndtert identisk som det var en helt ny bruker som vill ha den aktuelle siden. I forbindelse med innlogging, oppstod det et behov for å kunne avgjøre eller huske om personen som sendte forespørselen var en innlogget bruker. Rent teknisk ble dette løst i form av informasjonskapsler (cookies), som er en liten tekstfil lagret på brukerens harddisk og er tilknyttet en bestemt nettside. Nettstedet kan bruke denne lille tekstfilen til å skille mellom de forskjellige brukerene ved å lagre f.eks. en id. Informasjonskapselen vil bli sendt med når

brukeren etterspør en ny side, og dermed kan nettstedet avgjøre om brukeren er innlogget eller ikke. Informasjonskapsler ble introdusert som et tillegg til HTTP, for å kunne lagre tilstand [21] [22].

Den vanligste mekanismene for autentisering på nettsteder, er brukernavn og passord. Nettstedet har lagret en database som inneholder brukernavn, passord og annen informasjon for alle brukere. For å logge seg inn oppgir brukeren sitt brukernavn og passord, og nettstedet sjekker om brukernavnet finnes og det oppgitte passordet er korrekt. Når brukeren så oppgir brukernavn og passord sjekker tjener at dette finnes i systemet og gir i så fall brukeren tilgang.

2.4.6 Nye medier

De siste årene har det blitt et mye større fokus på brukergenerert innhold på nettsteder og brukeres interaksjon med hverandre. Enkelte mener at dette er en så stor forskjell fra tidligere nettsider, at et nytt begrep kreves; web 2.0. Andre mener begrepet er for vagt til å ha en formell definisjon, men vi kan generelt si at Web 2.0 kombinerer interaksjon, nettsamfunn og åpenhet [26]. Mens tidlige nettsteder for det meste inneholdt presentasjon av innhold eller kunne bli sett på som digitale brosjyrer, tillater nyere nettsteder at brukere kan komme med tilbakemelding eller kommentarer direkte på sidene. På den annen side er ikke dette unikt for nyere nettsteder, siden f.eks. Amazon har hatt brukeranmeldelser lenge før Web 2.0 var et begrep. Enkelte nettsteder tar i større grad rollen som et rammeverk, der brukere selv kan fylle inn innholdet.

Et kjennetegn for nye medier er at de i mye større grad legger til rette for flerveiskommunikasjon enn tidligere [14]. For tradisjonelle medier er skillet mellom sender og mottaker mye tydeligere. I nyere medier bidrar flere parter, og det er vanskeligere å skille mellom sender og mottaker. En måte å beskrive det er at alle involverte veksler på å være sender og mottaker avhengig av situasjonen. Hannemyr [14] argumenterer for at brukerne av nye medier ikke lenger kan sees på som kun mottaker, men mer som deltaker siden de også er med å produsere innhold.

Millard og Ross [26] har sett på om en rekke nettsteder kategorisert som Web 2.0 oppfyller forventningene til pionerene innenfor hypertekst. De konkluderer med at mange av ideene bak hypertekst har blitt realisert, men som applikasjoner på toppen av veven, ikke som et omspennende hypertekstsystem. Det er også enkelte aspekter av i tilfeller hvor de virker overflødige. Et eksempel som brukes er at wikisider er versjonerte, mens bloggartikler ikke er det. Det kan virke som om web 2.0 bevisst har avvist enkelte av de eldre ideene og forutsetningene knyttet til dem, til fordel for en lettere og mer

fleksibel fremgangsmåte. På samme måte som Internett, gjør dette web 2.0 mer evolusjonert hvor nye tjenester kan utvikles og legges til. Millard og Ross [26] mener derfor at web 2.0 kan sees på som en oppdatert visjon som løser noen av problemene som hypertekst skulle adressere.

O'Reilly [36] ser ikke på på web 2.0 som et konsept med faste rammer, men snarere en kjerne omkranset av en rekke begreper og konsepter. De utgjør ulike bestandeler av web 2.0, men alle trenger ikke være med for å kunne klassifisere et nettsted som del av web 2.0. O'Reilly [36] argumenterer samtidig for at "2.0-heten" ikke er noe nytt i seg selv, men snarere en følge av at vi har innsett potensialet i veven som en plattform. Vi har per i dag fått bedre innsikt i hvordan applikasjoner og tjenester utvikles for denne plattformen, sammenlignet med materiale som ble direkte overført fra andre medier i verdensvevens begynnelse.

Brukerene har tatt i bruk de nye løsningene og tjenestene og bruker dem for å utveksle informasjon eller holde kontakten med andre. Siden de fleste nettsteder gjør det mulig å melde seg inn og legge igjen kommentarer, ender brukere opp med å være registrert flere steder enn tidligere. Denne utvikling og ideene rundt samsvarer med Shneidermans tanker om "new computing" [45], at vi burde fokuserer mer på hva mennesker kan gjøre enn hva datamaskiner kan gjøre. Fokus på teknologi for å løse menneskers behov, kunne bidra til mer nyttig teknologi. Mange brukere er ikke interessert i teknologien som sådan, men mest opptatt av å kunne bruke den til å finne informasjon eller holde kontakten med venner og familie. Fortsatt er det stort sett brukernavn og passord som benyttes på sider hvor det er behov for å autentisere seg på nettstedene. Hovedforskjellen er at brukere er medlemmer av et stadig økende antall nettsteder for å holde konkakten med venner og familie, nettbutikker, interesser, hobbyer og mye annet.

Det er også interesse for sky-tjenester, der brukere benytter applikasjoner i nettleseren eller over nettet og informasjonen lagres på en ekstern tjener. På samme måte som terminalene koblet seg opp mot eksterne tjenere, er dette en ny bølge der lagringen av informasjon og kjøring av applikasjoner skjer eksternt. Også her finnes det en rekke forskjellige tjenester brukere kan forholde seg til, som igjen betyr et større antall brukernavn og passord.

2.4.7 Nye metoder for interaksjon

Over tid har vi gått vekk fra kommandolinjen til grafiske brukergrensesnitt, hvor alt er synlig og det er mulig å få umiddelbar tilbakemelding [35]. I tillegg til et større fokus på tjenester på nett, åpner også nye måter for interaksjon opp muligheter for grenesnittene vi benytter. Grensesnitt som bevegelser, posisjon og andre fysiske aspekter har til en viss grad blitt tatt

i bruk, og vil sannsynligvis gjøre seg mer gjeldende i fremtiden. Istedenfor dagens skjermer med tastatur og pekeredskaper, vil vi kunne ha flere fysiske enheter som legger til rette for bruk av touch eller andre metoder. I større grad tar vi i bruk mobile enheter som smarttelefoner, bærbare datamaskiner, lesebrett og nettbrett. Flere enheter som alle er koblet til Internett, som gir tilgang til forskjellige tjenester.

Naturlige brukergrensesnitt er en fellesbetegnelse for grensesnitt der interaksjonen foregår ved bruk av håndgrep, bevegelser o.l. En av grunnene til det grafiske brukergrensesnittets suksess er ifølge Norman [34] at det gjør det lettere å huske handlinger, både hvilke som er tilgjengelige og hvordan de utføres. Blant mekanismene for dette er synlige ikoner og menyer. Gjennom synligheten blir systemet utforskbart som gjør at brukere kan lettere navigere det for å finne funksjonaliteten de leter etter.

For et system basert på håndgester, er ikke nødvendigvis alle like utforskbart eller naturlige bevegelser. En rekke gester for å signalisere ulik betydning er også ulik for forskjellige kulturer. Norman peker også på at systemene gir lite informasjon når feil gest utføres, eller det ikke registreres hva som blir gjort feil. Brukere får få tilbakemeldinger når de utfører gestene, og ingen spor etterlates slik at det er mulig å se hvordan noe ble gjort i ettertid. Selv om Norman er enig i at gester kan være en god metode for interaksjon, har de fortsatt enkelte problemer. Vi mangler også en klar standard eller oversikt over mulige gester for å kunne gjøre mer enn det som er tilgjengelig per i dag. Som ved andre former for interaksjon vil brukere trenge en mental modell for hvordan de skal forholde seg til systemet, og hvilke konsekvenser forskjellig interaksjon vil føre til. Samtidig trengs måter å tilby tilbakemeldinger som beskriver mulig handlinger, og hvordan handlingene skal utføres riktig. Norman argumenterer at siden gester ikke har noen restriksjoner og dermed kan bli tvetydige eller svake, er det viktig at systemet kan gi tilbakemeldinger til brukeren om korrekt bruk av gestene. Norman konkluderer med at selv om det er misvisende å kalle interaksjon naturlig, siden bruk av tastatur, mus, eller gester alle er tillært, men de er likevel nyttige.

2.5 Design

For å designe et system i forhold til de behov og krav brukere har, trenger designeren ha detaljert kunnskap om brukeren og brukergruppen [32]. Hvis systemet kun skal benyttes av spesifikke brukergrupper, er det mulig å gå i dybden for å finne ut hva brukerene er ute etter. Hvis det derimot er tiltenkt å kunne brukes av alle, argumenterer Norman [32] for at å gå i dybden neppe er den beste fremgangsmåten. Når brukergruppen blir stor nok, vil overlappene mellom brukerne bli mindre, og det blir vanskeligere å legge til rette for hver

enkelt. For å utvikle et design for alle, kan det være mer hensiktsmessig å legge til rette for aktiviteter enn brukere.

Norman [32] sammenligner designet av systemer med hvordan hageverktøy eller kjøkkenredskaper har blitt utviklet. Slike verktøy har enkelte forskjeller fra kultur til kultur, men vil generelt være mer like enn ulike. Mye av grunnen er at de ble designet for å løse en oppgave, ikke utifra en brukersentrert studie. Deretter ble de forbedret over generasjonene basert på tilbakemeldinger og behov som ble adressert, som over tid gjorde verktøyene bedre egnet for større brukergrupper. Designeren kunne forme verktøyet ved å bruke sin forståelse av oppgaven det var ment for, og brukerene kunne forstå oppgaven og designerens intensjoner. Suksessfulle systemer er de som passer inn i kravene til den underliggende aktiviteten. Ved å forstå aktiviteten som skal utføres blir også redskapet forståelig.

En av farene med brukersentrert design er at i arbeidet med å tilpasse til en brukergruppe, blir det samtidig vanskeligere for en annen brukergruppe [32]. Å følge opp en spesifikk målgruppe over tid og legge designet bedre til rette for dem vil kunne gjøre verktøyet bedre egnet for denne gruppen. Men samtidig kan det føre til at verktøyet blir unødvendig komplekst og nærmest utilgjengelig for andre. Ved å istedenfor fokusere på aktiviteten, kan designeren unngå å ekskludere brukergrupper. Norman [32] ønsker likevel ikke å avfeie brukersentrert design, siden det fortsatt kan være et viktig verktøy for å avdekke hvilke områder som skaper problemer og således kan bidra til å forbedre designet.

Ifølge Norman [31] består forståelsen av en gjenstand brukeren møter på av tre elementer; konseptuelle modeller, begrensninger og tilbydelser. Valg av den konseptuelle modellen som skal brukes er en viktig del av designet. En passende modell skal velges ut, som skal være gjennomført og konsistent. Begrensinger har stort sett blitt ignorert som en del av et design [31].

2.5.1 Tilbydelser (affordance)

Affordance er opprinnelig et engelsk begrep som er vanskelig å oversette til norsk, men et tilsvarende begrep er tilbydelser [16]. Med bakgrunn i hvordan de er utformet, legger forskjellige gjenstander til rette for eller tilbyr visser former for bruk. Tilbydelser er egenskapene til en gjenstand [2], og hvilke handlinger den legger opp til mellom verden og en deltager [31].

Tilbydelser er et av aspektene som i stor grad gir brukerene et inntrykk av hva slags interaksjon som er mulig med grensesnittet. Elementer som benytter kan gi indikasjoner på hva som er mulig; knapper kan klikkes på, knotter kan skrus, o.l. Grensesnittet vil dermed gi hint om hvordan det kan brukes og hva det kan brukes til. Ved å aktivt utnytte tilbydelser kan designet formes

slik at brukeren vet hva som kan gjøres ved å se på det, uten at bruk av instruksjoner eller lignende er nødvendig. Baecker et al [2] bemerker likvel at for mer komplekse ting kan det være nødvendig med instruksjoner, men for enkle skal ikke trenges.

Det kan være nødvendig å skille mellom de faktiske tilbydelsene og de brukeren oppfatter [31]. Som et eksempel vil en skjerm potensielt kunne benytte touch siden det er mulig å ta på den, men det behøver ikke si at applikasjonene nødvendigvis støtter touch. Egenskapene skjermen har kan lede brukeren til å tro at de kan manipuleres via interaksjon, og det er viktig at designet ikke villeder brukeren. Derfor er samspillet mellom tilbydelser og tilbakemeldinger brukeren får svært viktig.

2.5.2 Tilbakemelding

Tilbakemelding, eller feedback, er den informasjonen som gis tilbake til brukeren basert på eller som et resultat av handlinger som har blitt utført. Når en handling endrer tilstanden i et system, er det viktig at brukeren ser endringen har funnet sted. Ved å bli presentert tilbakemeldingen kan brukeren se hva som skjedde og hvilke endringer som fant sted. Dix et al [7] beskriver to mulige varianter; automatisk vise resultatet av handlingen med en gang eller før eller senere. I beste fall kommer tilbakemeldingen på handlingen som ble utført automatisk uten at brukeren trenger å gjøre noe ytterligere. En annen løsning er å vise brukeren hva den gjeldende tilstanden er, når personen aktivt etterspør den. Ulempen med denne varianten er at brukeren ikke nødvendigvis vet hvor tilstanden kan sjekkes og dermed ikke får gjort det. Alt i alt bør umiddelbar tilbakemelding vises der det er mulig, og ellers designe systemet slik at brukeren vil kunne se hvilke endringer som har funnet sted.

Basert på brukerens inndata viser systemet tilbakemeldinger for å vise hva som ble registrert og hvordan det forandret systemet. Typisk tilbakemelding under innlogging er en melding som sier "vent litt" som vises etter at brukeren har skrevet inn passordet. Systemet signaliserer at det har registrert hva brukeren har skrevet og at det kontrollerer om det er riktig passord. Avhengig av hva brukeren har skrevet vil personen få videre tilbakemelding i form av å bli logget inn, eller en beskjed om at passordet er ugyldig. I begge tilfeller kan brukeren klart se hvordan systemet reagerer, og eventuelt hva brukeren må gjøre videre.

2.5.3 Metaforer

Metaforer benyttes for å kunne skildre noe ved hjelp av noe annet. Ifølge Preece et al [40] består grafiske brukergrensesnitt av elektroniske motparter

til fysiske objekter i den virkelige verden. Et av de fremste eksemplene innen HCI er skrivebordsmetaforen, som er bygget opp som et fysisk skrivebord med filer og mapper, som brukerne allerede kjente til. Ved å bruke metaforer i utformingen av et system, vil brukeren kunne forstå den nye systemet ved å lene seg på tidligere kunnskap fra områder brukeren allerede kjenner til [2]. I møte med nye systemer tar vi i bruk de erfaringer og kunnskap vi har med oss fra tidligere systemer. Hvis brukeren kan assosiere det nye systemet med noe brukeren allerede kjenner til blir det enklere å bli kjent med systemet, og forutse hvordan det fungerer i bruk.

Metaforer inneholder elementer og relasjoner mellom dem. De inneholder også forskjellige assosiasjoner som påvirker hvordan vi snakker og tenker om et gitt konsept [2]. Ved å bruke elementene fra et annet domene, kan brukere overføre de relasjonene elementene har mellom seg, slik at de i større grad er i stand til å forutse hvordan systemet vil reagere.

Preece et al. [40] skiller mellom verbale og virtuelle grensesnittmetaforer. Verbale metaforer baserer seg på å bruke deler fra et annet domene for at brukeren skal kunne kjenne seg igjen. Virtuelle grensesnittmetaforer går lengre, og legger opp til at hele systemet er utformet som noe i den virkelige verden. Dette gjør at brukeren kan danne seg en mental modell i forhold til hvordan den virkelige verden fungerer, ikke nødvendigvis hvordan det underliggende systemet utfører oppgaver. I slike tilfeller vil brukere i større grad vil utvikle funksjonelle mentale modeller, og være uvitende om de underliggende strukturene i systemet. Baecker et al. [2] mener også at metaforer kan bidra til at kjente, konkrete objekter og erfaringer gir mer struktur til abstrakte konsepter. Begge deler kan være ønskelige i enkelte tilfeller hvor de underliggende strukturene er kompliserte eller innfløkte, og det vil være enklere for brukerene å ha en enklere modell å forholde seg til.

Når designeren skal finne gode metaforer til et system, anbefaler Baecker et al [2] å identifisere mulige kandidater og så se i hvor stor grad de overlapper med oppgavene brukeren skal utføre. Spesielt er det viktig å identifisere mulige mismatcher, der systemet vil oppføre seg forskjellig fra hva metaforen kan antyde. Hvis mismatcher blir funnet tidlig, kan designeren finne metoder som hjelper brukeren å unngå problemene eller jobbe rundt dem. Hvis mismatchene ikke blir endret kan det hende brukeren oppfatter eller tyder hvordan programmet fungerer på en annen måte, enn det som var ment. Ifølge Baecker et al [2] er de fleste problemene brukerne har med metaforer ofte forårsaket av forskjellene mellom systemet og hvordan det fungerer i den virkelige verden, ikke på grunn av metaforen i seg selv.

2.5.4 Mentale modeller

Mentale modeller er brukerens egen modeller for hvordan et system er bygget opp og fungerer. Generelt danner mennesker seg representasjoner i forhold til seg selv, andre, objekter og miljøet rundt for å hjelpe dem vite hva de skal gjøre nå og i fremtiden [40]. I forhold til interaksjon med datamaskiner, kan modellene hjelpe brukere forme en abstraksjon av den underliggende arkitekturen og strukturen i programvaren, de konseptuelle entitetene som er implementert, som brukeren kan forstå [2].

Ved å analysere hvordan brukere forstår og utforsker systemet, kan denne kunnskapen benyttes til å designe grensesnitt som bedre støtter opp under de mentale modellene. Mentale modeller deles ofte i tre; den brukere har av systemet, hvordan det faktisk fungerer, og hva designere forsøkte å få frem. For å kunne utnytte de mentale modellene best mulig bør systemet legges tettest opp mot hvordan brukeren og designeren oppfatter systemet [43]. Suksessen blir på mange måter en følge av hvor godt brukerens modeller overlapper med hvordan systemet er konstruert [2]. Saei et al [43] argumenterer derfor for at de mentale modellene bør reflektere hva systemet inneholder, hvordan det fungerer og hvorfor det fungerer på den måten.

De mentale modellene tar i utgangspunkt tidligere erfaringer, men i motsetning til en prosedyre som følges slavisk kan modellene justeres [40]. I komplekse situasjoner vil brukere ha muligheten til å justere hvordan de utfører en oppgave. Basert på tidligere erfaringer er det også mulig å forstå nye oppgaver brukeren ikke har blitt utsatt for tidligere. Dette leder til mer fleksibel oppførsel, og det er antatt at de mentale modellene er basert på lagrede instruksjoner, men blir konstruert dynamisk ved behov. Modellene hjelper brukeren forutsi hvordan systemet reagerer på en en viss kommando, og for å kunne forutsi statusen til systemet etter et visst sett kommandoer [2].

Begrepet mentale modeller stammer opprinnelig fra kognitiv psykologi, som forsøker å forklare hvordan mennesker løser oppgaver de skal gjøre, men blir også benyttet i kognitive rammeverk innenfor HCI for hvordan vi tilegner oss kunnskap [40]. Tidlige modeller fremstilte mennesker som informasjonsbehandler. Mennesker som ble utsatt for inndata, ville prosessere den, sammenligne den med noe de kjente fra før, ta en avgjørelse basert på hva som skulle gjøres og utføre den handlingen. Opprinnelig på 1940-tallet, ble begrepet brukt for å beskrive hvordan vi tenker i form av en modell eller alternativ virkelighet for å prøve ut handlinger og forsøke å forutse resultatet før vi forsøker det samme i den virkelige verden. Tidlig på 1980-tallet ble to hovedtyper for mentale modeller identifisert; strukturelle og funksjonelle. Preece et al [40] definerer strukturelle modeller som en modell der brukeren er stand til å huske hvordan en enhet eller system fungerer, mens en funk-

sjonell modell tar utgangspunkt i at brukeren har kunnskap om hvordan å bruke systemet.

Strukturelle modeller innenfor HCI inneholder forenkleringer om hvordan systemet er bygget opp. Det er begrenset hvor nyttig disse modellene er siden de ikke nødvendigvis vil påvirke valgene brukeren tar. Det er likevel et interessant punkt om brukere danner seg en modell av systemet eller ikke. Derimot er de funksjonelle metodene viktigere, siden de vil ha en direkte innvirkning på hvordan brukere går frem i bruken av systemet.

Generelt tyder forskningen på at folk benytter seg av en mental modell i interaksjon med et system, men ofte er den vag og mangelfull. Systemdokumentasjonen forklarer ikke de mentale modellene for brukeren [2], så de må selv konstruere sine egne modeller for systemet. En grunn til at modellene ofte er ufullstendige, er at brukere ikke har en fullstendig oversikt over hvordan systemet fungerer [7]. Siden brukeren ikke har tenkt gjennom alle konsekvensene av hvordan de ser systemet, kan deler av modellen være ukonsistent med andre deler.

Som forklart over, kan de mentale modellene videreutvikles eller justeres etter hvert som brukeren utforsker programmet. Men de kan også justeres for å håndtere eller rette feil. Under bruk kan brukere lage sine modeller basert på egne myter og teorier om hvordan systemet er bygget opp. Disse antagelsene kan være feil eller misledende utenfor den begrensede situasjonen hvor de oppstod. Men hvis brukeren oppdager noe som fungerer annerledes enn forventet, vil modellen for programmet kunne endres til hva som faktisk skjer. Brukeren vil da ha en klarere modell for hvordan den aktuelle handlingen foregår i systemet for å kunne unngå nye feil i fremtiden.

Innenfor HCI har det blitt ansett som en fordel å designe systemet slik at det hjelper brukeren danne en mental modell, men til tross for dette finnes det lite konkrete fremgangsmåter for å designe for bedre mentale modeller [40]. Baecker et al [2] argumenterer for å designe modeller rundt oppgavene brukere skal utføre før systemet designes. Ved å sette fokus på oppgavene vil modellene kunne holdes under kontroll, enkle, konsistente og klare nok for brukerne. Designeres oppgave bør være å gi brukeren en eksplisitt modell som er lett å lære gjennom bruk av systemet. Om det er denne modellen brukeren ender opp vil bli påvirket av hvor klart den er implementert og hvor dokumentert den er.

2.6 Design og sikkerhet

Sikkerhet er et vanskelig område, også innen design. Whitten og Tygar [49] hevder en av hovedgrunnene er at sikkerhet ofte blir sett på som et underordnet mål. Brukere er mer interesserte i å bruke systemet til de oppgavene

de skal, enn at det er sikkert. Fra brukerens synspunkt gjør dette det mindre aktuelt å bruke tid på å sette seg inn i sikre løsninger, siden det vil stjele tid som heller kunne blitt brukt til å utføre arbeidsoppgavene. Det kan dermed ikke forventes at brukere tar seg tid til å lese lange instruksjonshefter eller på annen måte aktivt går inn for å øke sikkerheten [49]. En konsekvens kan være at bruker utsetter å sette seg inn i sikre løsninger.

2.6.1 Modeller for sikkerhet

På tross av at sikkerhet ofte ender opp som en baktanke når prioriteten er å utføre en oppgave, betyr det ikke at brukere ikke bryr seg om sikkerheten. Tvert imot uttrykker de fleste at de er opptatte av sikkerhet og personvern [4]. Så selv om brukerene ser behovet, kan det virke som det ikke blir fulgt opp i tilstrekkelig grad.

Camp [4] mener noe av grunnen er at det har vært for lite fokus på å kommunisere risiko. Hvis brukere ikke er klar over risikoene de utsetter seg for, sjansen for at det rammer dem, eller hvordan truslene sprer seg kommer de til å fatte sikkerhetstiltak basert på feil grunnlag. Ved å bedre presentere risikoene, kan brukerene få et bedre grunnlag. Camp [4] har sett på ulike mentale modeller for å bedre kunne kommunisere mulige risikoer, og kom frem til at den medisinske modellen kan være den beste modellen. Å trekke inn hvordan trusler kan spre seg, og gode forhåndsregler for å unngå å bli rammet vil begge være mulig å kommunisere i kontekst av systemer. Ved gi tilby en modell eller referanseramme brukere kjenner fra før, kan det påvirke dem til å bli mer bevisste på sikkerheten.

2.6.2 Tilbakemelding og sikkerhet

Sikkerhet er et område hvor det er vanskelig å gi gode tilbakemeldinger til brukere [49]. Det underliggende systemet er ofte komplekst og en kort oppsummering av tilstanden kan være mangelfull eller i verste fall villedende. Det kan også være vanskelig å avgjøre hva det er brukeren vil.

Pötzsch et al [39] gjennomførte en studie som viser at tilbakemelding vedrørende personvernrelaterte elementer gjør forumbrukere mer oppmerksomme på personvern. Det tyder også på at å være oppmerksomheten rundt personvern øker brukerenes kunnskaper om personlig data og gjør dem bedre i stand til å anslå hvor mange som kan se informasjonen de poster. De fleste brukerne i undersøkelsen oppga at de var klare over personvernproblematikken. Likevel kan Pötzsch et al [39] vise til litteratur som bygger opp under at brukere er mer åpne når det kommer til datasystemer enn i virkeligheten og at de overvurderer personvernet og gradvis blir mer åpne.

I en samtale med noen er det mye enklere å bedømme hvem som kan høre den i forhold til når noe publiseres på et nettsted. Pötzsch et al [39] la i undersøkelsene til tilbakemelding på et forum med ulike grader av opplysninger for at brukere bedre skulle kunne bedømme publikummet. På forumet ble det lagt til hint om at alle innlegg brukeren skrev ville være synlige på Internett, kombinert med besøkstall for forrige uke. Det ble også vist hvilken byen brukeren var i, i tillegg til IP-adresse, men sted ble ansett som mer forståelig for de som ikke var kjent med IP. Brukerne ble tilfeldig plassert i en av fire grupper. Den første gruppen ble kun vist de numeriske tilbakemeldingene, den andre ble vist kun tekstlige tilbakemeldingene, mens den tredje ble vist begge. Den fjerde gruppen fungerte som kontrollgruppe og ble vist reklame istedenfor.

Resultatene fra undersøkelsen viste at brukere som ble presentert hint følte de hadde mindre personvern enn de som ikke ble vist denne informasjonen. De så også at effekten var sterkere ved gruppene som ble vist en kombinasjon eller bare numerisk informasjon. Det var uklart om brukere som ble informert var i bedre stand til å bedømme hvor stort potensielle publikummet var. Ulike grader av tilbakemelding påvirket brukerenes oppfatning. På samme måte kan det tenkes at bedre tilbakemeldinger for andre aspekter innen sikkerhet gjør brukere bedre i stand til å selv bedømme sikkerheten.

De fleste moderne mobiltelefoner har støtte for GPS-teknologi, som har ført til at posisjonsbaserte tjenester har blitt mer utbredte. En studie gjennomført av Tsai et al [48] ønsket å se hvor viktig tilbakemelding var i forhold til personvernet i slike systemer. Mange systemer og tjenester finnes, men brukerne får lite eller ingen tilbakemelding om hvem eller hvor mange som har sett informasjonen de legger ut. I systemet for deling av posisjon via mobiltelefonen i undersøkelsen, hadde brukerne tilgang til et kontrollpanel der de kunne angi hvilke perioder i form av dager og tidspunkter andre skulle ha tilgang til posisjonen deres. Når andre brukere ber om tilgang til brukerens posisjon, blir det sjekket om tidspunktet er innenfor de tillatte grensene. Deltagerne ble delt i to grupper og fulgt opp ved å motta påminnelser via e-post. Den ene gruppen fikk tilbakemelding med oversikt over forespørsler, mens den andre gruppen ikke fikk tilbakemelding. Alle forespørsler som ble foretatt ble logget og var tilgjengelig for de som fikk se loggen sin. For hver forespørsel kunne de se hvem det var, når den var foretatt og om den hadde blitt godkjent eller ikke.

Resultatene viste at brukere som fikk tilbakemelding, var mer komfortable med å dele posisjonen sin, og brukte i større grad regler som gjorde posisjonen tilgjengelig i større tidsrom. Brukerene likte de tidsbaserte reglene for å begrense tilgang, men etterspurte også regler for å kontrollere tilgang til bestemte posisjoner eller grupper med brukere. Sannsynligvis ønsker de

mer finjusterte regler for å kunne vise posisjon for enkelte brukere men ikke alle.

Generelt er folk motvillige til å oppgi posisjonen sin, sannsynligvis på grunn av personvernhensyn. Dette er en mulig grunn til at slike tjenester hittil er lite utbredt. Tsai et al [48] argumenterer likevel for at også personvern tilpasser seg sosiale normer, slik at det er mulig det blir mer akseptert med tiden.

3 Metode

Denne delen forklarer valg av metoder, og beskriver de forskjellige. I arbeidet med oppgaven har en kombinasjon av metoder blitt benyttet; litteraturstudie, intervju og brukertest som hver skildrer forskjellige aspekter av problemstillingen.

3.1 Om valg av metoder

I arbeidet med oppgaven ønsket jeg å prøve ut noen av de forskjellige autentiseringsmekanismene med brukere for å se hvordan de fungerer i praksis. Jeg så for meg en veldig åpen studie, siden det er vanskelige å vurdere hvilke områder som er problematiske eller ikke på forhånd. Ofte håndterer brukere fint de elementene det var forventet var problematiske, mens de avdekker andre ting som ikke var forventet.

Før brukerne har bedømt systemet er det vanskelige å kjenne til mange kvalitetskrav for brukeropplevelsen. Cockburn [12] anbefaler derfor å ikke sette opp konkrete mål for å bedømme brukeropplevelsen, siden den ofte er vanskelig å måle ved hjelp av tall. Brukere ofte er usikre på hva de vil ha, så det er ofte bedre å ha et system som de kan kommentere å gå utifra, enn å sette opp en liste over krav før utviklingen har startet. Å studere interaksjonen brukerne faktisk har med systemet vil sannsynligvis gi mer relevant informasjon enn ved å skissere hvordan systemet skal legges opp. Cockburn [12] bemerker likevel at enkelte krav kan være delvis nyttige, som f.eks. hvor lang tid enkelte handlinger skal ta, er det mye mer verdifullt å se på de situasjoner og problemer som oppstår i praktisk bruk av systemet. Videre vil brukerenes kommentarer kunne gi ny innsikt i hvilke områder som trenger forbedring. Selv om de teoretiske målene er oppfylt, hjelper det lite hvis praksis viser at systemet er problematisk å benytte til å utføre de oppgaver det har blitt laget for. På bakgrunn av dette, har jeg valgt å studere hvordan de ulike mekanismene fungerer i bruk, fremfor å sette opp konkrete hypoteser på forhånd. Brukertesten vil derfor bli observert, men ikke med utgangspunkt i noen antagelser eller metrikker for forventede resultater på forhånd.

Cockburn [12] deler inn designelementer i tre kategorier; grunnleggende, lineære og spennende. Grunnleggende elementer er de delene som skal være til stede uansett, lineære er de som vil gjøre brukeren mer fornøyd desto flere som blir benyttet. Til slutt kommer de spennende elementene som brukeren vil like om er til stede, men ikke vil savne om de er fraværende. Ved å dele opp elementene på denne måten blir det mulig å kunne evaluere hvilke deler av rammeverket som er de viktigste og fokusere på disse elementene. Hvis

brukeren er fornøyd med utgangspunktet, er det mulig å gå videre og se på hva som kan legges til for å forbedre brukeropplevelsen på sikt.

For å teste brukeropplevelsen, skiller Mashapa og Greunen [25] mellom tre hovedmetoder; brukertester, ekspertvurderinger og undersøkelser. I brukertester får en gruppe vanlige brukere en liste over oppgaver de skal utføre i systemet de skal prøve ut. Mens de gjør oppgavene blir de observert hvordan de går frem, og om de er i stand til å løse de oppgavene de har fått. Det gjør det mulig å i stor grad se hvordan brukerne går frem og hvilke områder som skaper problemer. Mange brukertester benytter også "thinking aloud", som vil si at brukeren skal si hva personen tenker og forklare valgene personen gjør. I ekspertvurderinger vil en ekspert innen brukeropplevelser gå igjennom verktøyet eller prototypen og vurdere hvilke elementer som kan skape problemer. Eksperten har ofte mye erfaring fra lignende systemer eller brukeropplevelser generelt og vil kunne oppdage typiske problemer som brukere kan ha problemer med. Rene undersøkelser tar for seg meningene til brukerene, og kan hentes inn etter at brukerene har brukt systemet for å avdekke hvordan de oppfattet det og hva de synes var problematisk. Det kan være i form av spørreundersøkelser eller korte intervjuer, der brukerne selv kan vurdere og ta stilling til forskjellige aspekter ved systemet.

De forskjellige metodene kan kombineres, og denne oppgaven bruker en kombinasjon av brukertest og undersøkelse. Brukere skal teste ut ulike innloggingsmekanismer, mens de etter hver mekanisme skal svare på spørsmål om hvordan de oppfattet den. Prototypen de tester er meget minimalistisk og inneholder kun de grunnleggende elementene, som er de ulike autentiseringsmekanismene. Det kan likevel argumenteres at enkelte deler av instruksjonene eller tilbakemeldingene er lineære elementer som hjelper til. De er med andre ord ikke knyttet til noe system eller nettsted, men kun innloggingen har blitt skilt ut. Målet er å teste selve autentiseringsmekanismene uten for mange distraksjoner og andre elementer rundt. Dette betyr også at unødvendige elementer har blitt kuttet bort, slik at det er lettere å fokusere på de grunnleggende elementene. Hvis mekanismene virker lovende kan de integreres og bli tatt i bruk av ulike tjenester eller systemer. Hvis de derimot er problematiske for brukere alene bør de enten forkastes eller i beste fall endres for å adressere problemene før de integreres som en del av større tjenester.

3.1.1 Andre metoder

Et eksperiment kunne gitt mer konkrete resultater, men krever strengere formelle krav for undersøkelse. I et eksperiment bør det være strengere kontroll over variablene som påvirker utfallet [37]. Det er også vanskelig å sette opp et eksperiment som ville vært reproduserbart, så en brukertest fungerer bedre

i dette tilfellet. For et eksperiment ville det også vært mer aktuelt å velge deltakere tilfeldig, fremfor å hente inn brukere fra spesifikke brukergrupper som er gjort her.

Siden brukerundersøkelsen vil ha et begrenset antall deltakere, gir kvantitative metoder som spørreundersøkelser lite mening. For en representativ spørreundersøkelse ville det vært nødvendig å hente inn data fra et større antall respondenter. På grunnlag av svarene, vill det vært mulig å trekke konklusjoner for resten av befolkningen. En naturlig forutsetning her er selvsagt at de som har svart er representative for den øvrige befolkningen. Slike undersøkelser brukes ofte for å finne ut hva den generelle befolkningen mener om noe, hvor det er relevant å studere en større gruppe mennesker. Med et lite utvalg personer, vil det ikke være mulig å kunne si noe generelt hverken om befolkningen eller om spesifikke brukergrupper. Jeg har derfor valgt å fokusere på kvalitative metoder, som egner seg bedre for et mindre antall deltakere.

3.2 Litteraturstudie

Med utgangspunkt i eksisterende litteratur vil problemstillingen diskuteres i forhold til de resultatene jeg finner. Først og fremst vil litteraturen bidra med hvilke autentiseringsmekanismer som finnes og har blitt sett på tidligere. Særlig studere som allerede har sammenlignet flere lignende mekanismer og sett på fordeler og ulemper er aktuelle. Det er også aktuelt med litteratur innenfor menneske-maskin interaksjon i tillegg til sikkerhet, siden jeg ønsker å ta for meg begge fagfelt. Fra designsiden blir det viktig å trekke inn teknikker eller konsepter som er aktuelle i utformingen av autentiseringsmekanismer eller i forhold til de mentale modellene brukerne danner seg under bruk.

I utgangspunktet så jeg på mer generelle aspekter ved innlogging, men begynte etter hvert å fokusere mer på konkrete deler. Jeg benyttet primært artikler publisert av ACM og IEEE, så vel som utvalgte bøker om enkelte emner. Gjennom søk fant jeg flere artikler som berørte samme tema, og som kunne benyttes i sammenheng. I noen tilfeller oppdaget jeg også artikler som ble refert ofte, eller virket interessante å se nærmere på. Alt i alt fant jeg et godt grunnlag for å kunne diskutere de forskjellige aspektene av problemstillingen, som også etter hvert ble mer konkretisert. Ved gjennomgang av ulike autentiseringsmekanismer, oppdaget jeg at det har blitt gjort mye arbeid innenfor feltet. Siden det ville blitt for omfattende å dekke alle mekanismer som har blitt forsøkt, valgte jeg å heller satse på et utvalg av autentiseringsmekanismer som har blitt undersøkt tidligere. Deler av utvalget omfattet også mekanismer som var inkludert i prototypen eller var nært beslektet, noe som gjorde det enklere å kunne trekke linjer videre til mekanismene der.

3.3 Brukerundersøkelse

Jeg så tidlig for å meg å ha brukerundersøkelse som en del av oppgaven, og se hvordan brukere opplever og håndterer ulike autentiseringsmekanismer. Vel så viktig som det teoretiske fundamentet for ulike mekanismer for innlogging er det å kunne studere dem og se hvilke problemer eller utfordringer som oppstår ved bruk. Det gjør det mulig å se om det er forskjeller ved ulike mekanismer, og høre med brukere hvilke tanker de gjør seg om dem. Jeg valgte å se på en brukertest der brukere prøver ut ulike mekanismer siden dette kan si noe om hvilke problemer og syn brukere har på forskjellige innloggingsmekanismer.

Målet her er ikke å kunne trekke konklusjoner basert på et representativt utvalg av befolkningen, men snarere å eksplorativt se hvordan ulike brukergrupper reagerer på de ulike mekanismene. Det ble heller ikke satt opp hypoteser eller teorier på forhånd om de ulike mekanismene, siden fokus var på å se hvilke mekanismer som kan brukes og hvordan de fungerer. For senere tester eller undersøkelser kan det være mer interessant å se på mer konkrete hypoteser om hvilke mekanismer som er foretrukket, eller lignende. Det er også mulig resultatene fra denne undersøkelsen da kan benyttes i arbeidet med videre hypoteser og undersøkelser senere. I utgangspunktet er målet å se hvilke mekanismer som kan brukes, og hvordan brukerne oppfatter dem.

I brukertestene vil autentiseringsmekanismene bli testet ut for seg før de blir hektet på en løsning. Testen brukere skal gå igjennom er med andre ord kun registrerings- og innloggingsfasen uten å være koblet til noe system eller tjeneste. Hovedgrunnen er for å kunne skille ut den delen som er aktuell for undersøkelsen uten at andre elementer skal kunne påvirke undersøkelsen. Det er også i tråd med Cockburns tanker om å teste de grunnleggende elementene av designet før andre elementer legges til. Det gjør det mulig å bedømme og vurdere hvordan mekanismene fungerer alene.

Flere metoder for brukertesting tar utgangspunkt i at en flere personer vil samlet avdekke flere problemer i et program eller nettsted en person alene vil gjøre. Nielsen [30] mener grunnen er at hver person kan peke ut et eller flere problemer hver. Samlet vil dette føre til enkelte overlappende rapporter om de samme problemer, men også enkelte problemer som bare en av personene finner vil avdekkes. Det vil være logisk å anta at et større antall personer som prøver ut løsningen gir et bedre resultat, men det er bare delvis korrekt. Nielsen har lengre erfaring med heuristiske evalueringer med ulike antall deltakere, og har kommet frem til at flere personer vil kun lede til at flere problemer avdekkes opp til et viss punkt. Når metningspunktet er nådd vil de fleste personene i hovedsak finne kjente problemer. Dette innebærer få nye resultater, samt i tillegg brukes mye tid og energi på de ekstra personene.

Det er heller nyttigere å utbedre de problemene som har blitt avdekket og gjenta evalueringen på et senere tidspunkt for å se etter nye feil. Brukertesten fokuserer derfor på et lite antall deltakere (fem), men de vil likevel trolig kunne avdekke de fleste problemene.

3.4 Gjennomføring av brukerundersøkelse

I undersøkelsen skal hver bruker gå gjennom registrering og innlogging med fem forskjellige mekanismene og vurdere dem. Brukeren vil bli stilt spørsmål etter hver mekanisme, og det er en helhetsvurdering til slutt. Mekanismene er samlet på et nettsted, så alt brukeren trenger er en datamaskin med en nettleser. Sammen med brukeren er testleder som også stiller spørsmål underveis, eller kan hjelpe brukeren hvis personen står fast eller lurer på noe. I tillegg er det en til to observatører til stede (inkludert meg), for å observere hva brukeren gjør.

På forhånd ble brukerne tilsendt et skriv med informasjon om selve testen og hvordan personvern vil bli ivaretatt siden informasjon tilknyttet brukerene vil bli lagret. Før selve brukertesten startet, ble brukeren blir introdusert til systemet og oppgavene. Testlederen går kort igjennom hvordan testen er lagt opp. Informasjonen fra infoskrivet blir repetert, og brukeren blir fortalt at testen vil bli tatt opp på bånd. Før brukeren kom, har testlederen satt opp en tilfeldig rekkefølge for de ulike mekanismene som brukeren skal gå igjennom.

Hoveddelen av testen, er at brukeren går igjennom hver mekanisme på egenhånd. Observatørene legger merke til og noterer oppførsel eller andre interessante hendelser. Hvis brukeren står fast, kan testlederen hjelpe brukeren videre ved å komme med forslag eller hint. Etter registrering har brukeren tre forsøk på å logge seg inn med mekanismen. Hvis brukeren logger inn på disse forsøkene, regnes mekanismen som vellykket fullført. Hvis derimot ikke brukeren får logget seg inn går systemet videre etter de tre forsøkene er brukt opp, og mekanismen regnes som gjennomført. Etter hver mekanisme blir brukeren vist status for hvor langt personen har kommet i testen, med hvilke mekanismer som er fullført, om de var vellykket eller ikke og hvilke som gjenstår.

Etter hver mekanisme stilles brukeren et sett med spørsmål. De tar for seg hvordan brukeren likte mekanismen, og om det var noe som var vanskelig underveis. De fleste spørsmålene er åpne, men enkelte benytter seg av en Likert skala for å vurdere mekanismene i forhold til om brukeren likte dem godt, meget godt, ikke så godt eller likte dem dårlig. Testlederen fulgte også opp med tilleggsspørsmål for temaer brukerne tok opp eller for å utdype svarene. Spørsmålene som ble brukt er lagt ved i Appendiks A. De samme spørsmålene gjentas for hver mekanisme, for å få brukerens vurdering mens

mekanismen fortsatt er friskt i minnet. Ved å få umiddelbar tilbakemelding, får heller ikke senere mekanismer noen fordel. Hvis vurderingene hadde blitt samlet til slutt, ville senere mekanismer være friskere i minnet enn de tidligste, som kunne påvirket resultatet. Etter å ha svart på alle spørsmålene, går brukeren videre til neste mekanisme.

Etter å ha vært innom alle mekanismene blir brukeren bedt om å rangere alle mekanismene. Rangeringen foregår ved at brukeren gir hver mekanisme en poengsum fra en til fem, hvor fem er best. Brukeren kan gi samme antall poeng til mer enn en mekanisme. Deretter stiller testlederen ytterligere spørsmål om mekanismene. Disse spørsmålene er beregnet for mer inngående diskusjon og vurdering av de forskjellige mekanismene opp mot hverandre, hvem brukerne likte best og hvorfor. Brukerne ble også spurt om å vurdere hvilke trusler brukeren ser på som aktuelle mot de forskjellige mekanismer. Spørsmålene er lagt ved i Appendiks B. Testlederen kan også spørre om andre ting, som problemer som oppstod eller andre valg brukeren gjorde underveis.

3.5 Blikksporing

Forskjellige verktøy kan benyttes under brukerundersøkelser for å bedre dokumentere nøyaktig hva brukeren foretar seg. Et verktøyene som kan benyttes er blikksporing, som kan hjelpe til med å se hvor problemer oppstår eller om elementer er plassert feil. Ved hjelp av spesialutstyr kan testen bruke en skjerm som er i stand til å følge øynene til brukeren og registrere hva personen ser på, samt hvor lenge blikket holder seg på et sted. I forhold til ren observasjon er blikksporing å foretrekke, siden ren observasjon kan føre til misoppfattelser, og er vanskeligere å dokumentere eller vise til i ettertid. Ved å samle en fullstendig logg vil det også være mulig å oppdage mønstre som kommer klarere frem i ettertid som kanskje ikke blir registrert ved å observere brukeren under selve testen.

Før selve testen må systemet kalibreres for hver enkelt bruker ved hjelp av enkle tester der de skal følge en peker med blikket og lignende oppgaver. Brukertesten foregår ellers som normalt, hvor brukerne går igjennom og gjør de oppgavene de skal. Mens testen foregår, blir brukerens handlinger registrert og lagret.

Ved å studere opptaket senere, er det mulig å se hvordan brukerens blikk flyttet seg mens testen ble gjennomført. Spesielt interessant er det å kunne studere hvilke deler av skjermen brukeren fokuserte på for å se om brukeren la merke til informasjonen eller overså deler, og i tilfeller hvor problemer oppstod. Mulig grunner til at blikket holdes i visse områder kan være at det som befinner seg i området er interessant eller at bruker ikke vet eller forstår hva personen skal gjøre. Det gjøre det også mulig å se nærmere på steder

brukeren hadde problemer i ettertid for å få en bedre oversikt over hva som skapte problemer og hva brukeren gjorde. Samtidig er det mulig å se hvor mye av den tilgjengelige informasjonen brukeren får med seg, eller om det bør vurderes å flytte den til et annet område for at brukeren bedre skal legge merke til den. Det er også mulig å få en oversikt over hvilke områder av skjermen brukeren så mest på, ved hjelp av fargemarkeringer.

4 Case

Denne delen av oppgaven beskriver hvordan brukertesten var lagt opp, samt forskningsprosjektet den var knyttet til.

Brukertesten har blitt gjennomført innenfor forskningsprosjektet e-Me i perioden jeg har skrevet oppgaven min. Jeg har fått bli med e-Me både på møter og planlegging av brukertestene, samt vært med som observatør.

4.1 e-Me

e-Me er et prosjekt, med fokus på metoder for innlogging, tilgjengelighet og sikkerhetsløsninger. Noe av det de ser på er måter for brukere å håndtere sin digitale identitet, og alternative autentiseringsmekanismer som kan passe for ulike brukergrupper er et av aspektene som er interessant her. Prosjektet ble startet våren 2010, og vil gå frem til utgangen av 2013. Deltakerne i prosjektet kommer fra bla. Norsk regnesentral, Universitet i Oslo, Karde AS og Tellu AS. I tillegg har de avtaler med organisasjoner og firmaer som representerer både utviklere, tjenestetilbydere men også brukergrupper.

Et av målene med prosjektet er å se på forskjellige autentiseringsmekanismer som kan benyttes med tanke på å legge til rette for flest mulige og de ulike brukernes behov. Enkelte sikkerhetsmekanismer kan by på utfordringer for enkelte brukergrupper, og prosjektet ønsker å kunne legge bedre til rette for å identifisere og løse disse utfordringene. Det er både fokus på problemer med mekanismer som er i bruk, men også hvilke alternativer som kan tilbys i tillegg eller som en erstatning for tradisjonelle mekanismer. Selv om noen mekanismer fungerer bra for enkelte, kan de være utfordrende eller umulig for andre brukergrupper.

Prosjektets innhold spenner seg fra utvikling av prototyper, testing med brukere, vurdering av brukers behov og av tilgjengelighet ved de forskjellige mekanismene. Målet er å bedre forstå utfordringer brukere har med ulike autentiseringsmekanismer og hvilke alternativer som kan passe for ulike brukergrupper. Noe av tanken bak er å ikke nødvendigvis finne den ene mekanismen som kan benyttes av alle, men heller se hvilke mekanismer som kan passe for ulike brukergrupper.

4.2 Prototypen

Prototypen som blir benyttet inneholder en rekke forskjellige autentiseringsmekanismer og har blitt utviklet for e-Me for å kunne teste ut disse. Selv om det kunne vært fristende å se på eksisterende tjenester siden de allerede er kjent, er det mye vanskeligere å endre eller videreutvikle de fleste større

tjenester. Det ville blitt problematisk å endre detaljer eller legge til nye mekanismer, siden de har få eller ingen muligheter for tilpasning. Prosjektet valgte derfor å se bort fra eksisterende tjenester i denne omgang, og istedenfor sette opp sin egen prototype som fritt kan tilpasses. En annen fordel med å bruke et eget system, er at prosjektet vil ha full kontroll på alle data som registreres, og kan dermed ta bedre hensyn tildeltagernes personvern. Hvis et eksisterende sosialt nettsted hadde blitt benyttet, ville det vært mye mer betenkelig å registrere informasjonen der siden det er uvisst hvordan den vil bli benyttet. Ved å selv håndtere informasjonen, vil prosjektet kunne hindre at dataen som blir registrert ikke misbrukes til andre formål i ettertid. Det er også også mulig å slette dataen etter at eksperimentet er gjennomført, en mulighet som neppe ville vært der om en etablert tjeneste hadde blitt benyttet. To ulemper er at prosjektet ikke har et kjent, etablert system å lene seg på og at det krever mer utvikling på forhånd.

Den foreløpige prototypen har kun fokus på registrering og innlogging med de forskjellige mekanismene. Senere i prosjektet er det planlagt å koble mekanismene sammen med forskjellige tjenester og prøve ut i forhold til det, men for tiden er fokus kun på selve innloggingen alene. Prototypen inneholder følgende mekanismer; passord, bildegjenkjenning, gjenkjenning av lyd, personlige spørsmål og mønstergjenkjenning. Målet med prototypen er å se hvilke av mekanismene som skaper problemer for brukerne, og hvilke som kan benyttes i fremtiden.

Ved testing av prototypen er det mulig å observere hvordan de forskjellige mekanismene fungerer, hvor lang tid de enkelte tar og eventuelle problemer under innloggingsprosessen. Mekanismene skal testes med forskjellige brukergrupper, som gjør det mulig å se om det er enkelte som passer bedre for de ulike gruppene.

De ulike mekanismene blir presentert i en rekkefølge som blir bestemt før brukeren starter testen. For hver mekanisme går brukeren gjennom registrering og innlogging, før personen skal vurdere den. Hver mekanisme har informasjon om hvordan den fungerer og klare instruksjoner for hva brukeren skal foreta seg. Denne teksten presenteres slik at brukeren kan lese den før personen går i gang med selve registreringen. Tekstene inneholder korte forklaringer som beskriver hva brukeren skal gjøre skrevet med enkelt språk som skal gjøre det lett å forholde seg til og sette seg inn i. Avsnittene i teksten har fått begrenset bredden til maksimum 60 tegn for å gjør det lettere å følge setningene, spesielt for dyslektikere. Prototypen inneholder heller ingen urolige bilder eller rare farger blir benyttet, og jevnt over forsøkt å få et renest mulig grensesnitt slik at det er mulig å fokusere på mekanismene i bruk.

For å eliminere unødvendige elementer og redusere tiden det tar å gjennomføre en test har behovet for registrering blitt redusert til et minimum.

Brukerne slipper å forholde seg til brukernavn, som blir lagt inn av testleder før testen starter. Dermed slipper brukerene å bruke tid på å skrive inn fullt navn og annen informasjon, som ikke er relevant for å teste de forskjellige autentiseringsmekanismene.

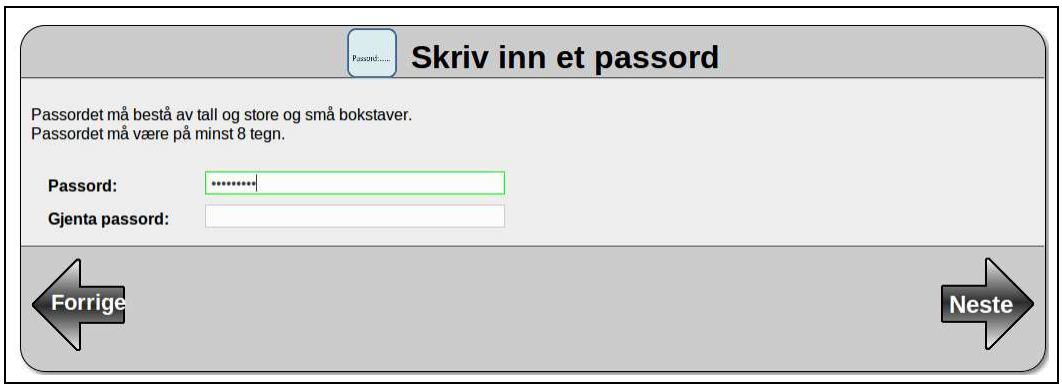
For hver gang bruker går videre til neste ledd i prosessen, trykker personen på en knapp merket "neste" nederst på skjermen. Mellom registreringen og innloggingen er det et klart skille med et skjermbilde som forklarer at brukeren skal benytte informasjonen som nettopp ble registrert for å logge seg inn. Mellom hver mekanisme blir brukeren vist status, som gir tilbakemelding på hvilke mekanismer som har blitt gjennomført, om de var vellykket eller ikke og hvilke som gjenstår. Mekanismene vises i samme rekkefølge som brukeren tester de i.

Etter å ha gått igjennom alle mekanismene, skal brukeren rangere dem ved å gi dem poeng, og gi en helhetlig vurdering av dem. Mekanismene blir listet opp i den rekkefølgen brukeren gikk gjennom dem med både navnet og et ikon for å representere dem. Ved siden av er et lite tekstfelt der brukeren kan skrive inn en poengsum mellom en og fem for å rangere mekanismene, basert på hvem brukeren likte best.

4.3 Brukertest

Prototypen brukes som en del av brukertesten. Formålet er å se hvordan de ulike mekanismene fungerer i praksis med reelle brukere. Brukerne skal teste ut de forskjellige mekanismene, mens de blir observert for å se om det er problemområder eller elementer ved de forskjellige mekanismene som bør endres. Det legges også vekt på hvordan brukerne oppfatter de forskjellige mekanismene, hvilke de foretrekker og hvorfor. Hvordan selve testen blir gjennomført er beskrevet i detalj i kapitlet om metoder.

Før brukertestene ble en pilottest gjennomført, for å se om testen var for omfattende ved at den inneholdt for mye på en gang eller tok for lang tid. En annen grunn var for å avdekke umiddelbare problemer i prototypen som bør utbedres, siden dette var første gangen noen som ikke var involvert i forskningsprosjektet fikk prøve ut prototypen. En person var deltager i pilottesten, og flere problemer ble avdekket og rettet før selve brukertesten. Resultatene fra piloten, samt endringene som ble gjort i ettertid er tatt med og beskrevet blant funnene fra undersøkelsen.



Figur 1: Registrering av passord

4.4 Autentiseringsmekanismene

4.4.1 Passord

Passord er den tradisjonelle mekanismen for autentisering, og går ut på at brukeren oppgir en hemmelig kombinasjon av bokstaver, tall og tegn for å logge seg inn. Den er likevel inkludert både for å kunne sammenligne den med de andre mekanismene, men også for å se hva brukerne mener om passord. Selv om målet i hovedsak er å se på alternativer til passord, er det samtidig interessant å kunne sammenligne, og se hvilke områder som er problematiske i forhold til de andre.

Brukeren får instruksjoner for hvordan passordet skal være utformet, inkludert krav om blanding av store/små bokstaver og tall og at passordet skal ha en viss minimumslengde. Ved registrering skal brukeren skal skrive inn passordet to ganger, den første gangen for å angi sitt passord, og den andre for å bekrefte det og kontrollere at de er like slik at det er riktig skrevet. Ved innlogging skal brukeren oppgi passordet sitt igjen for å logge seg inn. Passordene blir skjult og erstattet med stjerner (*) for at ikke andre skal kunne se hva brukeren skriver på skjermen.

4.4.2 Bildegjenkjenning

Noen brukere, spesielt dyslektikere har vanskeligheter med å huske lengre og kompliserte passord. For disse brukerene kan det være enklere å huske bilder fremfor passord. Ved registrering velger brukeren seg et visst antall bilder fra en oversikt med et større utvalg av forskjellige bilder og symboler.

Ved registrering velger brukeren seg fem bilder av totalt 60 tilgjengelige. Brukere skal så huske de fem bildene og benytte seg av dem for å logge inn

Figur 2: Registrering av bilder

senere.

Ved innlogging blir brukeren presentert for ti ulike bilder, der et av dem er tilfeldig valgt fra de opprinnelige fem. Brukeren skal finne sitt bilde og velge det for å logge seg inn. For å øke sikkerheten og gjøre det vanskeligere for andre å gjette brukerens bilde blir tre ulike sett vist etter tur. De to andre fungerer likt som det første, men med andre bilder. Hvis alle tre bildene som ble valgt er korrekte har brukeren logget seg inn. Hvis et eller flere var feil, må brukeren starte på nytt og brukeren får beskjed om at ikke alle bildene var riktige. Det blir ikke oppgitt hvor mange, eller hvilket bilde brukeren valgte som var feil, siden det ville gjort det enklere for andre å gjette seg frem til de riktige bildene.

4.4.3 Gjenkjenning av lyd

For blinde og sterkt svaksynte kan grafiske løsninger som passord og bildegjenkjenning være vanskelige å bruke. For disse kan det være nyttig å kunne logge seg inn ved hjelp av et antall lyder brukeren husker. Denne mekanismen kan også være aktuell for andre brukergrupper.

Ved registrering velger brukeren et antall lyder fra et utvalg. I prototypen skal brukeren velge fem lyder fra et utvalg på rundt 60, fordelt på fire

Figur 3: Registrering av lyder

kategorier. Kategoriene deler lydene naturlig inn i dyrelyder, generelle lyder, sanger, og musikkinstrumenter. Lydene vises sammen med et abstrakt bilde som representerer lyden, for å kunne gi assosiasjoner og forsterke inntrykket. Dette vil kunne gjøre det enklere å velge og kjenne igjen lydene. På venstre-siden vises fire abstrakte bilder som symboliserer de forskjellige kategoriene. Brukeren kan veksle mellom kategoriene ved å klikke på en av de andre. Den gjeldende kategorien blir vist med samme bakgrunnsfarge som lydutvalget, mens de øvrige kategoriene har en lysere bakgrunnsfarge.

De fleste lydene er hentet fra ulike lydbiblioteker. For denne undersøkelsen ble det også benyttet musikk som brukerene vil kunne kjenne igjen. For en tjeneste i den virkelige verden, ville det neppe vært gjennomførbart med tanke på opphavsrett og rettigheter. Det er fortsatt et kategori som vil kunne benyttes, gitt at tjenesten har de tilstrekkelige rettighetene til å benytte klippene som skal brukes. Siden synshemmede kan være mer vare for kraftige lydinntrykk, ble enkelte av lydene endret slik at de ikke kom med skarpe eller

brå lyder når brukeren forsøkte å merke dem.

Under innlogging blir brukeren presentert 10 forskjellige lyder der en er tilfeldig valgt fra brukerens lyder. Brukeren skal velge sine lyder for å logge seg inn. I likhet med bildegjenkjenning blir dette gjentatt tre ganger med ulike lyder, for å være sikker på at det er den rettmessige brukeren som logger seg inn og ikke noen som gjettet hvilken lyd som var den riktige. Etter å ha valgt alle tre lydene blir brukeren logget inn. Hvis brukeren har valgt en eller flere feil lyder, blir brukeren informert om dette og må starte på nytt.

Figur 4: Registrering av spørsmål og svar

4.4.4 Personlige spørsmål og svar

Personlige spørsmål baserer seg på at brukeren husker et antall personlige spørsmål og svar. Brukeren blir presentert spørsmål, og oppgir de korrekte svarene for å logge inn. Siden spørsmålene er personlige, vil ikke uvedkommende kjenne svaret.

Under registrering oppgir brukeren et antall personlige spørsmål. Prototypen har enkelte forslag (som navnet på bestefaren din), og andre spørsmål som typisk blir brukt i lignende tjenester. Det er også mulig å legge til sine egne spørsmål hvis brukeren ønsker det. Brukeren blir instruert at spørsmålene

skal være personlige slik at kun de vil vite svaret, de har også mulighet til å legge til hint for svaret. Brukeren skal fylle inn minimum fem spørsmål og svar. Underveis kan brukeren se en oversikt over hvor mange spørsmål som har blitt lagt til hittil, og brukeren kan ikke gå videre før minimum fem spørsmål har blitt lagt til. Denne oversikten tilbyr også muligheten til å slette eller redigere spørsmålene som har blitt lagt til.

Ved innlogging blir brukeren presentert et av spørsmålene, og skal oppgi svaret. Hvis et hint ble oppgitt under registreringen er dette tilgjengelig, og vil bli vist under spørsmålsteksten. Ved å oppgi et svar, går brukeren videre til et nytt spørsmål. Spørsmålene blir valgt tilfeldig fra brukerens spørsmål, og brukeren må svare korrekt på tre spørsmål for å kunne logge seg inn. Hvis brukeren har glemt svaret, eller ønsker å svare på et annet, er det mulig å hoppe til et annet spørsmål. Da byttes spørsmålsteksten ut med et annet tilfeldig valgt spørsmål fra de brukeren har registrert. Brukeren må likevel svare på totalt samme antall spørsmål. Hvis et eller flere av svarene på spørsmålene er galt får ikke brukeren vite det før alle tre spørsmålene er besvart. Brukeren blir da informert om at et eller flere svar var galt, og må begynne på nytt.

Figur 5: Registrering av mønster

4.4.5 Mønstergjenkjenning

Mønstergjenkjenning fungerer ved at brukeren husker et mønster og tegner det i et rutenett ved innlogging.

Under registrering kan brukeren selv tegne opp et mønster i et rutenett på fem ganger fem ruter. Mønsteret skal inneholde minst fem ruter, men det er ingen begrensninger på maksimum. Brukeren avgjør selv hvor avansert mønsteret skal være. Nedenfor rutenettet er det en knapp for å nullstille rutenettet for å kunne begynne å tegne på nytt.

Ved innlogging skal brukeren tegne opp det samme mønsteret som ble personen oppgav under registrering. Også her er det en knapp tilgjengelig for å starte tegning av mønsteret på nytt.

4.4.6 Mobiltelefon

Prototypen har støtte for autentisering via mobiltelefon, men denne mekanismen ble ikke benyttet i brukertestene. Grunnen er at mekanismen er meget omfattende og ville tatt store deler av tiden i brukertesten, så den ble ikke sett på i denne omgang. Det ble heller prioritert å kunne se på et større antall mekanismer på en gang. Dermed utgår den inntil videre, men vil sannsynligvis bli sett nærmere på senere i prosjektet. Et lite program blir installert på brukerens mobiltelefon som gjør det mulig å logge inn på nettstedet.

Ved registrering oppgir brukeren telefonnummeret sitt og hvilken type telefon det er. Type er nødvendig for å kunne vite hvilken variant av programmet som skal benyttes, noe som vil variere i forhold til hva slags telefon brukeren har. Løsningen fungerer på telefoner som støtter Java, men også smarttelefoner med enten Android eller iOS. Sammen med programmet, mottar brukeren en kode som må tastes inn for å bekrefte at telefonen registreres til brukerprofilen. Hvis brukeren ønsker, kan programmet benytte en PIN-kode som er nødvendig for å låse opp programmet når det skal brukes. Brukeren angir selv PIN-koden som skal brukes, og må huske denne selv. Å benytte PIN er dog valgfritt, og brukere kan istedenfor velge å ha programmet tilgjengelig for alle som har fysisk tilgang til telefonen. Det sikrere alternativet er dog å kombinere telefonen (noe brukeren har) og PIN-koden (noe brukeren vet), istedenfor å begrense seg til kun telefonen. Ved å knytte telefonen til tjenesten, har telefonen nå blitt en kodebrikke, på samme måte som kodegeneratorer blir benyttet av banker.

Mens registreringen er komplisert, er mekanismen enkel i bruk. For å få tilgang til en tjeneste, oppgir brukeren brukernavnet sin til en tjeneste. Samtidig låser brukeren opp programmet på telefonen med PIN-koden (hvis nødvendig) og kjører programmet. Programmet på telefonen kommuniserer

med tjenesten, og brukeren vil bli logget inn. Hvis tjenesten ikke hører fra programmet innen kort tid (tre minutter i prototypen) etter at brukeren forsøkte å logge seg på, går tiden ut og brukeren vil måtte starte innloggingsprosessen på nytt.

5 Funn

Her presenteres de ulike resultatene fra brukertestene. Resultatene er fordelt etter de ulike mekanismene og evalueringen til slutt. For hver mekanisme blir det skildret hvordan brukerne gjorde det under registrering, innlogging og vurdering. Eventuelle problemer eller spørsmål brukerne hadde underveis er også dekket.

5.1 Forberedelser til brukertest

Undersøkelsen ble utført ved at brukere fikk prøve de forskjellige autentiseringsmekanismene. Resultatene jeg har er basert på brukertester som ble gjennomfør med fem seniorbrukere. Det er planlagt å gjennomgå samme undersøkelsen med fem dyslektikere og fem svaksynte eller blinde testpersoner senere i prosjektet. Jeg fikk være med og observere brukertestene, og resultatene er i stor grad basert på observasjonene og notatene jeg gjorde under testene.

Brukere som deltok i undersøkelsen var fem seniorer. Dette inkluderer en pilottest, hvor resultatene fra denne er også tatt med. For resultatene og diskusjonen videre vil de forskjellige personene omtales som P1 til og med P5, hvor P1 er piloten og P2-P5 er de øvrige personene.

Før brukerne startet satte testleder opp de forskjellige mekanismene i tilfeldig rekkefølge, for å unngå at resultatene påvirkes av tidligere mekanismer og jevne det ut mellom de ulike mekanismene. Siden enkelte mekanismer ligner på hverandre (som bilder og lyd), er det viktig å teste de i forskjellige rekkefølger siden erfaringene med bruk av den ene kan spille inn på den andre. Hvis brukeren f.eks. har problemer eller spørsmål til den første mekanismen, er det trolig brukeren ville hatt de samme problemene med den andre også. Siden brukeren allerede har fått svar på spørsmålene sine er det sannsynlig brukeren reagerer annerledes på mekanismen enn hvis personen ikke hadde sett noe lignende tidligere. Mange brukere sammenlignet også mekanismene underveis med andre de hadde prøvd tidligere, og i teksten har det blitt angitt hvilke mekanismer de sammenligner med.

Alt brukerene trengte for å gjennomføre testen var en datamaskin med nettleser og Internett-tilgang, siden prototypen befant seg på nettstedet til e-Me. På forhånd la testleder inn brukernavn for brukeren og en tilfeldig rekkefølge for mekanismene. Brukeren overtok deretter maskinen, og kunne etter å ha lest igjennom en kort introduksjon gå igang med første mekanisme. Brukerne ble oppfordret til å primært følge instruksjonene på skjermen, men også til å si ting høyt hvis de stod fast eller noe virket rart. Testpersonene er alle erfarne brukere, og det er mulig resultatene ville vært annerledes med

nybegynnere. Målet med undersøkelsen er likevel ikke å teste kunnskapen til brukerene, se hvordan de ulike mekanismene fungerer i praksis. Brukerne P1 og P2 gjennomførte testen i Norsk Regnesentral sine lokaler, for P3 og P4 ble testen gjennomført hjemme hos brukerne, mens P5 ble gjennomført hos Seniornett. Grunnet tekniske problemer benyttet P4 sin egen maskin. P5 benyttet også sin egen maskin.

I motsetning til hva som var planlagt, ble blikksporing dessverre ikke tatt i bruk. Hovedgrunnen var at den tekniske løsningen for blikksporing var bundet til en nettleser som hadde manglende støtte for enkelte deler av prototypen. Andre nettlesere som hadde full støtte for prototypen var ikke mulig å benytte til blikksporingen.

5.2 Pilottesten

Før pilottesten hadde de involverte i prosjektet gått igjennom og diskutert hva som skulle være med i prototypen og hvordan den skulle utformes. Enkelte elementer var mye diskutert, som inndelingen i kategorier for lyd og bilder. Etter å ha kommet frem til enighet om prototypen, rettet stavefeil og mindre problemer, ble prototypen testet ut med en pilot.

Pilottesten avdekket enkelte problemområder, som førte til endringer før de øvrige testene ble gjennomført. Resultatene fra pilottesten er likevel inkludert, og eventuelle forskjeller beskrevet i teksten. De to største endringene var for bilder og lyd. Bildene brukeren kunne velge mellom under registrering til bildegjenkjenning var i utgangspunktet delt inn i kategorier med mulighet til å veksle mellom de forskjellige via faner på toppen. Her ble kategoriene fjernet, og bildene vist samlet istedenfor. Om utvalgene skulle holdes samlet eller deles inn kategorier hadde blitt diskutert tidligere i prosjektet, men måten utvalget presenteres ble endret når det ble klart piloten hadde problemer med kategoriene. For lyder ble kategoriene likevel beholdt, slik at mekanismene var delt inn forskjellige for å mulig kunne se noe om hva brukerne foretrakk. I gjenkjenning av lyd ble også kategorien film byttet ut med musikkinstrumenter, basert på tilbakemelding fra piloten. Brukeren likte ikke kategorien film, siden brukeren ikke kjente til noen av lydene fra før. Dette var også et punkt som hadde blitt diskutert tidligere, og ble endret når det viste seg at piloten hadde lite kjennskap til filmene som var tatt med.

Mekanismene som gjorde det mulig å angre et utvalg av bilder, lyd eller mønster ble også gjort tydeligere etter pilot, og det ble klarere spesifisert at det var en mulighet. De valgte bildene eller lydene ble hele tiden vist i et felt nederst på skjermen. Over feltet var det en kort tekst som fortalte "trykk på et av bildene for å fjerne det". Slik teksten var skrevet kunne den oppfattes som en ordre, og brukeren i pilottesten ble veldig forvirret hvorfor bildene

som nettopp var blitt valgt skulle fjernes igjen. Teksten ble derfor endret slik at det skulle komme tydeligere frem at det var et valg som brukeren kunne gjøre, hvis personen angret eller ville gjøre om noe av utvalget. Det var også mulig å klikke på en lyd eller et bilde som allerede var valgt, for å velge det bort igjen. Teksten på angreknappen til mønster ble også endret for at det skulle komme klarere frem at det kun var en mulighet. Etter pilottesten, var det ingen av brukerne som benyttet seg av angreknappene eller utvalget som ble vist nederst. I tillegg ble andre mindre endringer gjort for å rette småfeil i tekstene eller for å gi klarere instruksjoner. Disse endringene er kommenterte hvor de er relevante.

5.3 Generelt

Generelt brukte noen av brukerene veldig kort tid på instruksjonene og det er usikkert om de leste eller fikk med seg alt. Etter at alt var blitt klargjort og datamaskinen overlatt til P5, trykket brukeren seg først videre uten å lese introduksjonen. Brukeren ble da minnet på at det var viktig å lese instruksjonene og gikk dermed tilbake igjen.

Sammen med instruksjonene til hver mekanisme, ble et lite ikon over for å symbolisere mekanismen. De samme ikonene ble senere brukt sammen med navnet på mekanismene til evalueringen, for å minne brukeren på hva de forskjellige mekanismene var. Når de kom til bildegjenkjenning ble det vist et ikon med fire bilder over instruksjonene. En del av brukerne forsøkte å klikke på ikonet, mulig fordi teksten beskrev de skulle velge forskjellige bilder. De fleste så derimot ut til å umiddelbart skjønne at ingenting skjedde og gikk dermed videre.

5.4 Passord

Etter å ha lest gjennom instruksjonene, spurte P1 om det var meningen at personen skulle huske passordet eller om det var mulig å notere det et sted. Da P5 kom til punktet hvor det stod det skulle velges et passord som må huskes, utbrøt personen "huffameg". Personen forklarte etterpå at personen hadde trodd det skulle være flere passord, og teste ut kombinasjoner av eller stokke dem.

5.4.1 Registrering

Under registreringen, telte P4 antall tegn i passordet for å forsikre seg om at det inneholdt åtte tegn. Samme person får ikke registrert passordet på første forsøk fordi passordet ikke inneholder to tall. Brukeren går da tilbake

til instruksjonene og begynner på nytt. Bemerker selv at personen overså at det skulle være to tall, og andre forsøk går fint.

P1 benyttet passordet som var oppgitt som et eksempel i instruksjonene. De øvrige brukerne registrerte et passord uten problemer.

5.4.2 Innlogging

Ved innlogging trengte P1 to forsøk for å logge inn. Personen fikk tilbakemelding om at passordet var feil etter første forsøk. Etter å ha kommentert dette selv, gikk personen videre og forsøkte å skrive inn passordet på nytt, som var vellykket. De øvrige brukerene logget seg alle inn på første forsøk.

5.4.3 Vurdering

Passord var middels godt likt. P1 anså mekanismen som grei, mens P2 synes den var meget god. P3 mener passord forsåvidt er godt nok, men var ikke den mekanismen brukeren likte best. Sistnevnte utdypet svaret sitt med at personen forsåvidt likte passord, men synes det er vanskeligere å huske enn personlige spørsmål. Hovedgrunnen var at det ikke er nødvendig å bruke mye energi på å huske personlige ting som f.eks. hva moren din heter. P5 mener passord er lette å huske, men kommenterte også underveis at personen synes bilder var en morsommere og enklere metode.

P4 synes passord er en grei metode, og bemerker det er samme som benyttes på nettsteder eller til bank. Brukeren regner med den må være sikker siden den er mye brukt. P5 kommenterte også at det er en vanlig mekanisme.

Av egne passord oppga flere av brukerene (P2, P4 og P5) at de var vant med kombinasjoner av tall og bokstaver fra tidligere. P2 mente det eneste nye her sannsynligvis var kombinasjonen med små og store bokstaver, som brukeren ikke var vant til fra tidligere. P5 synes kombinasjonene gjør passordet mer komplisert å huske.

Mange brukere sier de foretrekker å ha et system for passordene sine, som gjør det enklere å huske. Som P2 sa, blir det enklere ved å ha noen knagger å henge det på. Flere av personene har et system basert på navn i kombinasjon med fødselsdato eller en datoer for begivenheter personen husker. De fleste har stor tiltro til systemene sine, og P3 bemerker at de er basert på noe personen ikke kommer til å glemme. P3 kommenterte også at personen benytter seg av ulike passord, som endres og utvikles over tid ved at nye tegn blir lagt til. “Hvis det var hjemme ville jeg skrevet det opp”, sa P2 underveis, og forklarte at personen har passord nedskrevet i tilfelle personen glemmer dem.

Blant instruksjonene var det inkludert et eksempel på et passord som oppfylte retningslinjene med blanding av store og små bokstaver og tall. Eksemplet brukt var en gateadresse. En av brukerne, P1, oppfattet at dette passordet skulle benyttes. Under vurderingen etterpå, oppga likevel P1 å ha en oppfattelse av at passord er noe som velges slik at en selv kan huske det. P5 valgte også å bruke en adresse som passord, men i motsetning til P1 valgte personen en annen adresse enn den oppgitt i eksemplet. Når personen ble spurt etterpå, svarte personen at adressen ble valgt fordi det var mulig, ikke fordi vedkommende oppfattet det var det man skulle. Personen la deretter til at personen ikke ville brukt et slikt passord i virkeligheten.

5.5 Bildegjenkjenning

Under pilottesten var P1 meget forvirret og forstod lite av denne mekanismen. Brukeren var spesielt usikker på hvor mange og hvordan bilder skulle velges. I utgangspunktet var ordlyden i teksten at brukere skulle velge bilder, men det var ikke spesifisert hvordan velgingen skulle foregå. P1 oppfattet at personen skulle plukke ut enkelte bilder, og noterte seg disse. Under piloten ble personen først hintet tilbake til beskrivelsen, før det ble forklart at formålet var å klikke på bildene for å velge dem. Teksten ble senere endret for å tydeligere spesifisere at bilder ble valgt ved å klikke på dem.

5.5.1 Registrering

Bildeutvalget var i utgangspunktet delt i flere kategorier, men dette ble endret etter piloten. P1 forsøkte å velge et bilde fra hver kategori, og det var flere kategorier enn bilder som skulle velges. Etter å ha vurdert problemene under piloten, ble utvalget endret til å samle alle bildene og tilby et rullefelt for at brukerne skal kunne bla gjennom de forskjellige bildene.

De fleste brukerne studerte bildene før de valgte seg ut fem stykker og gikk videre. Ingen så ut til å ha noen problemer med å bla opp eller ned i vinduet for å kunne se resten av bildene. Enkelte brukere, som P2 og P4, kommenterte begge at det var veldig mange bilder når de fikk se utvalget. P4 bemerket også at personen ikke hadde noen preferanser for valg av bilder. Flere brukere inkluderte det norske flagget i bildeutvalget.

P2 valgte et bilde, valgte det så bort igjen, før personen gikk tilbake til instruksjonene og så frem igjen. P2 kommenterte så at personen glemte å lese teksten, og valgte bilder.

5.5.2 Innlogging

Alle brukerne unntatt P4 logget inn på første forsøk uten problemer. P4 lurte først på om bildene måtte tas i samme rekkefølge, hvorpå brukeren ble oppfordret til å følge instruksjonene. Brukeren logget seg dermed rett inn. P5 spurte først om flere bilder brukeren hadde valgt ble vist, men oppdaget ved å se nærmere at kun et av bildene var der.

5.5.3 Vurdering

Jevnt over synes P1 hele mekanismen virket diffus. Spesielt hadde brukeren problemer med å velge bilder, som under piloten ikke var beskrevet klart nok hvordan bilder skulle gjøres. P2 og P3 likte heller ikke mekanismen så godt, og sistnevnte var usikker på om personen ville klare å huske alle fem bildene.

Enkelte av brukerne kommenterte at det var veldig mange bilder når de fikk se utvalget. P2 kommenterte der var nødvendig med flere bilder for å gjøre det vanskeligere for andre, mens P1 lurte på hvorfor så mange bilder var tatt med, og ble forklart at et større utvalg gjør løsningen sikrere.

Brukerne hadde forskjellige fremgangsmåter for å velge bilder. Siden piloten inneholdt kategorien, valgte P1 bilder fra ulike kategorier. P2 valgte bilder litt tilfeldig, så på forskjellige bilder, og valgte ut de som ville være mulige å huske. P3 valgte bilder utifra hva som var enklest å huske, og så ikke på alle. P5 valgte seg bilder personen forbandt med personlige hendelser, for å lettere kunne huske dem. Personen mente at med et såpass bra utvalg burde alle kunne finne bilder de forbandt med noe. P5 likte også at mekanismen var rask, og satte pris på at det var mulig å bare klikke seg gjennom.

Ingen av brukerene i undersøkelsen så ut til å ha noe problemer med å bla opp og ned på siden, men P3 mislikte det. Personen synes selv ikke det var problematisk, men likte ikke at det var nødvendig. Etter å ha gått igjennom en lignende mekanisme tidligere og fått svar på spørsmål der, synes P5 det var enklere å gå gjennom denne mekanismen.

Med tanke på sikkerhet, anså P4 bildegjenkjenning som en veldig god mekanisme som er vanskelig for andre å gjette. Brukeren bemerket dog at enkelte brukere kan bli forvirret av mange bilder på en gang. Sammenlignet med andre mekanismer mente P2 at bilder var mer tungvint enn passord siden det var mer å huske på, mens P5 synes bilder passet bedre enn spørsmål. P5 tror bilder er en mekanisme som kan passe bra for eldre, kanskje folk generelt. P2 mener at bruk av bilder kan være en god ide, men at det trolig vil fungere bedre etter å ha innarbeidet det en stund.

5.6 Gjenkjenning av lyd

Etter at personen hadde lest instruksjonene var P5 undrende til at det ble anbefalt å velge lyder fra forskjellige kategorier. En kort pause oppstod da P5 begynte med denne mekanismen, for å få skrudd på høyttalerne og justert volumet slik at brukeren kunne høre lydene. Vi tror ikke dette påvirket inntrykket av mekanismen.

5.6.1 Registrering

I likhet med bilder, valgte P1 å notere lyder fremfor å klikke på dem. Etter å ha notert flere lyder, oppfattet brukeren at også her skulle det klikkes på de forskjellige lydene som tidligere. I forhold til hvor mange lyder som skulle velges var P1 usikker, siden det var færre kategorier enn lyder som skulle velges. Etter å ha valgt ut en lyd fra hver kategori, manglet brukeren fortsatt en i forhold til antall lyder som skulle velges. Under valg av bilder, hadde også brukeren forsøkt å velge et bilde fra hver kategori.

Kategoriene var problematisk for brukerene. Ingen av brukerene bortsett fra P1 oppfattet hvordan det var mulig å veksle mellom de forskjellige kategoriene. De andre brukerene endte derfor alle opp med å kun velge lyder fra den første kategorien, som var dyrelyder. P2 uttalte i ettertid at personen hadde stusset over bildene til venstre, men var ikke klar over at de var til å velge andre kategorier.

Under registreringen hørte P2 på forskjellige lyder og så seg rundt. Gikk så tilbake til instruksjonene, før personen gikk frem igjen og valgte lyder. P4 hadde problemer med utvalget. Brukeren klikket først på en lyd og valgte den uten problemer, men brukte så en stund på å holde markøren over andre lyder før det gikk opp for brukeren også de andre lydene måtte klikkes på for å velge dem. P4 hadde litt problemer med å finne knappen for å gå videre først, men fant den raskt ved å bla ned.

5.6.2 Innlogging

Når brukerne kom til innloggingen, logget P2 og P5 rett inn uten problemer. P3 forsøkte under første innloggingsforsøk å trykke på andre lyder. Dette var en bevisst handling fra brukerens side for å se hva som skjedde hvis andre lyder ble valgt under innlogging. Brukeren kommenterte så at teksten over riktignok kun sier "Velg en lyd", og ikke at brukeren skal velge sine lyder. Brukeren mener dette er et punkt som andre kan misforstå og som derfor bør rettes. Andre forsøket går uten problemer.

P4 kommenterte at det var helt andre lyder ved innlogging. Brukeren valgte først en av lydene fra registreringen, men gikk deretter videre for å

velge flere lyder også her. Personen undret seg over at kun en lyd var valgt, enda flere hadde blitt klikket på. Brukeren måtte bli minnet om at under innlogging skulle kun en lyd velges, og at innloggingen spenner seg over flere steg. Etter å ha blitt informert om dette, forstod brukeren systemet og logget inn. P1 var også usikker under innloggingen på hvordan det var mulig å komme seg videre til neste steg. Personen utbrøt også på et tidspunkt at ingen av de tilgjengelige lydene var noen av dem som hadde blitt valgt tidligere, men fikk til slutt valgt den riktige og kom seg videre.

5.6.3 Vurdering

Veldig få likte denne mekanismen. P1 vurderte mekanismen til midt på treet, P2 og P5 likte den ikke så godt, mens P3 mente det var den dårligste mekanismen personen hadde forsøkt hittil. Flere som hadde prøvd bilder tidligere, mente mekanismen var veldig lik, men med lyd i tillegg. P1 var usikker på hvorfor lyd skulle benyttes til innlogging, og P5 så heller ingen gevinst ved å bruke lyd. Sistnevnte lurte på om det var muligheter for å kun høre lydene uten bildene, og kjenne dem igjen basert på det.

Siden kun en bruker valgte lyder fra flere kategorier, endte de andre brukerene opp med å velge bare dyrelyder. P1 valgte lyder med utgangspunkt i hva personen trodde han ville huske senere. P3 valgte klare lyder, mens P4 brukte et system for å assosiere lydene til noe. Sistnevnte mente det var vanskelig å huske noe uten system, og mente fem lyder kunne bli litt mye. Brukeren foreslo et bruke færre antall lyder istedenfor, f.eks. tre, og ønsket også å kunne skrive ned eller assosiere lydene med noe.

Mekanismen var grei å forstå ifølge P3, bortsett fra instruksjonene ved innlogging som personen bemerket tidligere. P5 synes også mekanismen var litt vanskelig å forstå, og merket seg at instruksjonene anbefalte å velge lyder fra flere kategorier uten at brukeren benyttet seg av dette.

En av brukerene hadde en del meninger om mekanismen. P3 synes den var morsom, men samtidig at det var litt barnslig at den gir lyd. Siden brukeren ikke så på de andre kategoriene under registrering er det vanskelig å anslå hvordan disse kunne påvirket vurderingen. P3 nevnte også at mekanismen ikke er særlig praktisk hvis andre er i nærheten og kan høre det. Personen lurte også på hvordan det går hvis brukeren trenger høyreapparat.

Alt i alt synes P5 lyder var veldig lik bilder, men foretrakk sistnevnte, siden personen gikk etter bildet fremfor lyden. Personen bemerket at det kanskje ikke var poenget med mekanismen. P2 likte heller ikke lyden og ville oretrukket kun bilder, men trodde det ville blitt enklere etter å ha brukt mekanismen noen ganger. Etter å ha lest instruksjonene først hadde P5 heller sett for seg at man fikk høre en lyd og så skulle finne bildet som hørte til.

5.7 Personlige spørsmål og svar

Før brukeren gikk i gang med registreringen, lurte P5 på hvor mange spørsmål som skulle legges til, og fikk til svar at det skulle personen kunne se.

5.7.1 Registrering

Flere av brukerene valgte en kombinasjon av å lage egne spørsmål og bruke de som allerede var tilgjengelige. P2 og P4 holdt seg til forhåndsdefinerte spørsmål og la ikke til egne siden de mente det ikke var nødvendig. P1 og P3 la hver til to egne spørsmål. Særlig P3 brukte lang tid på å legge til nye spørsmål og synes det var vanskelig å finne på nye spørsmål. Hovedgrunnen til at P3 valgte å legge til egne spørsmål, var at de forhåndsvalgte ikke passet. Etter å først ha lagt til fem forhåndsvalgte spørsmål etter hvert som de dukket opp, gikk P5 over til å legge til egne spørsmål. Siden brukeren på dette tidspunkt hadde det nødvendig antall spørsmål for å gå videre, hintet testleder til at brukeren skulle se på toppen av vinduet. Brukeren leste deler av teksten, og mente det var greit. Gikk så videre for å legge til enda et spørsmål. På dette tidspunktet ble det bemerket hvor mange spørsmål brukeren hadde laget og at det var mulig å gå videre, noe brukeren også gjorde.

På samme måte som brukerene valgte å legge til egne eller holde seg til spørsmålene angitt på forhånd, var det enkelte som la til hint, mens andre ikke gjorde det. P1 la til hint på sine spørsmål, P3 la til på kun et spørsmål (drøftes i detalj senere), P5 brukte hint på alle spørsmålene sine, mens P4 ikke brukte hint i det hele tatt. Grunnen til at P1 la til hint for sin egen del for å ha en måte å kunne komme tilbake til svaret. Også P5 oppga at grunnen var for å ha en måte å sette seg selv på sporet hvis personen hadde glemt svaret.

Mens brukerne forsøkte å registrere spørsmål dukket det etter hvert opp et par problemer, som de i stor grad klarte å løse på egenhånd. Det er usikkert hvordan mindre erfarne brukere ville håndtert problemene som oppstod underveis. Etter at P1 hadde valgt å oppgi sitt eget spørsmål, begynte brukeren å skrive på tastaturet selv om tekstboksen ikke var i fokus. Når brukeren så opp, merket personen selv at det ikke var blitt skrevet noe, klikket på ruten for å gi den fokus og skrev inn spørsmålet fra begynnelsen. P4 lurte på hva knappen merket "Legg til" gjorde og antok først den var knyttet til hintet, men kom etter å ha tenkt seg om frem til at det la til hele spørsmålet. For et spørsmål fylte også P4 inn svaret i tekstboksen for hintet istedenfor og forsøkte å legge til spørsmålet. Siden det ikke var lov til å spørsmål med tomme svar fikk brukeren tilbakemelding om dette fra systemet. Brukeren rettet opp dette selv, når personen oppdaget spørsmålet ikke var blitt lagt

til.

Både P3 og P4 bemerket at spørsmålet "Hva heter bestefaren din?" er upresist siden alle har to bestefedre. Dette var spørsmålet P3 la til et hint på, for å huske hvilken side navnet var fra.

Den eneste brukeren som nevnte muligheten for å endre eller slette noen av spørsmålene var P4, som kommenterte at disse spørsmålene skulle personen klare å huske. De andre personene benyttet ikke av disse mulighetene, og nevnte dem heller ikke.

5.7.2 Innlogging

Alle brukere logget vellykket inn på første forsøk. I ettertid kommenterte P3 at personen ikke visste hvor hint dukket opp under innlogging, men antok det kanskje ville dukket opp ved å trykke på knappen merket "husker ikke". Hint ble automatisk vist under spørsmålet, men med mindre skriftstørrelse og det er usikkert om de andre brukerene la merke til det heller.

5.7.3 Vurdering

De fleste brukerene likte mekanismen meget godt, unntatt P3 som synes den var god og P2 som ikke likte den så godt. De som likte den meget godt trakk frem at den var enkel å forstå, lett å komme på noe, lett å huske og det er veldig få andre som vil vite svarene på spørsmålene. P3 la særlig vekt på sikkerhetsvurdering og hvor trygg personen følte seg, og likte denne mekanismen bedre enn bilder. Hovedgrunnen til P2 sin misnøye var at det var veldig mye å gjøre, og mange operasjoner før det var mulig å logge seg. Det ble lagt opp til mer skriving og mer å svare på i forhold til f.eks. passord, og P2 kommenterte dette kan være et problem for brukere som har et problem med å skrive mye.

Flere av brukerene, bla. P1 og P5 bemerket de ikke var helt ukjente med denne mekanismen og at de hadde sett den i bruk i andre tjenester. P2 derimot hadde ikke vært borti denne mekanismen før.

Enkelte av brukerene valgte å legge til egne spørsmål, mens andre klarte seg med å velge blant de forhåndsdefinerte. For å forhindre at brukere la til egne spørsmål som var for enkle, foreslo P3 å legge til hjelp for å lage nye spørsmål. Hvis brukerene legger til for enkle spørsmål, blir det alt for lett for uvedkommende å gjette seg til svaret. P3 likte heller ikke spørsmål som baserte seg på nyere tid, siden svarene kan endre seg over tid. F.eks. la brukeren selv til spørsmålet "Hvem er din beste venn?" som personen i ettertid kommenterte kan endre seg etter hvert.

Flesteparten av brukerene mente instruksjonene var greie, P2 sa personen ikke lurte på noe underveis. P3 var litt usikker på hvor hint dukket opp under innloggingen. For P4 var instruksjonene greie, men brukeren lurte i ettertid på hvor mange ganger det er lov å svare feil ved innloggingen. P5 var litt usikker på forskjellen mellom forhåndsdefinerte spørsmål og egne og synes den delen var uklar. Brukeren hadde ikke oppfattet ordentlig at det var en grense på fem spørsmål.

5.8 Mønstergjenkjenning

Etter å ha lest instruksjonene kommenterte P1 at personen synes antall mønstre var uklart. Når personen kom videre til selve registreringen så personen dog ikke ut til å ha noen problemer.

Under piloten, ble P1 litt forvirret av knappen for å fjerne ruter, da den som for bilder og lyd var skrevet som en ordre. Personen ble forvirret over at det som hadde blitt tegnet opp skulle fjernes igjen. Teksten på knappen ble endret til den endelige versjonen, der det kom tydeligere frem at det var en angreknapp. Ingen brukere valgte å benytte seg av angreknappen, hverken under registrering eller innlogging.

5.8.1 Registrering

P4 bemerket tidlig at dette ville bli komplisert. Personen trengte et system for mønsteret, men ikke for komplisert slik at det var mulig å huske det.

Brukerne hadde ingen problemer med å komme på eller tegne mønstre, som hadde varierende kompleksitet. Alle brukere benyttet seg av minimum antall ruter som skulle fargelegges før de kunne gå videre. P1 og P2 tegnet begge veldig enkle mønstre med en enkel diagonal strek fra øvre venstre hjørne til nedre høyre hjørne. Sistnevnte så lenge på rutenettet før personen tegnet noe. P3 tegnet en pil som peker oppover, bestående av fem ruter. Mønstrene til P4 og P5 var mer avanserte. Mønsteret til P4 markerte en rute på hver rad, organisert systematisk basert på hvor langt unna kanten den valgte ruten var og på hvilken side den var plassert. P5 satt og tenkte en stund før personen tegnet et mønster, med enkeltruter tilsynelatende hver et stykke unna hverandre uten noen sammenheng. Når personen ble spurt etterpå, kom det frem at mønstret var basert på hvordan en springer beveger seg i sjakk, slik at brukeren ville kunne vite hvor det neste punktet i mønsteret er. Personen kom på systemet etter å ha sett rutenettet siden det minner om et sjakkbrett. Begge de to sistnevnte kommenterte at personen kun trengte å huske mønsteret for å vite hvor de skulle plasseres til innlogging.

Når P4 tegnet mønsteret sitt ble brukeren forvirret over at alle ruten ble blå, siden personen hadde sett for seg at flere farger ble benyttet. Personen forsøkte derfor å klikke på enkelte av rutene flere ganger for å se om de skiftet farge. Etter en stund ble brukeren forklart kun en farge ble brukt. Brukeren hadde regnet med at flere farger ble benyttet for å gi flere muligheter.

5.8.2 Innlogging

Alle brukerene logget seg inn vellykket på første forsøk. Ingen så ha ut til å ha noen problemer med å oppgi mønsteret sitt på nytt.

5.8.3 Vurdering

Flere av brukerne likte denne mekanismen. P2 synes den var meget god, mens P1 holdt seg til at den var grei. P4 foretrakk personlige spørsmål fremfor denne mekanismen. Selvom personen var enig i at mønstergjenkjenning er grei, synes ikke personen den var like bra. Til slutt synes P5 at denne mekanismen var morsom, uventet og meget enkel å utføre og likte den veldig bra, spesielt siden brukeren anser seg selv som en visuell person.

Selv om det virket som det var enkelte uklarheter basert på brukernes erfaringer, var de fleste enige om at mekanismen var grei å forstå. P5 bemerket at den krever at bruksanvisningen blir lest, men synes ellers den gikk fort og mente det var noe som var lett å huske. P1 var i utgangspunktet litt usikker på betydningen av mønster, men mente det gikk greit når man skjønner hva som skulle gjøres. Problemet brukeren hadde med angreknappen fra pilottesten ble rettet opp før de senere testene og ingen av de andre brukerene så ut til å ha samme problemet. P3 mente mekanismen var grei og skjønne, og likte at rutenettet ikke var for stort så det ble for uoversiktlig. P2 lurte heller ikke på noe undervis underveis. Personen mente mønstergjenkjenning var ukomplisert, og at det bare var å klikke i vei.

Mens P4 var litt forvirret over at det kun ble brukt en farge, synes P5 den var veldig klar, så fort brukeren fikk sortert ut at forskjellige farger ikke ble brukt. P5 la også til at personen likte at det ikke var forskjellige farger, kun fokus på selve mønsteret.

En del av brukerne valgte enkle mønstre og et mønster gikk igjen; en diagonal linje fra øvre venstre hjørne til nedre høyre hjørne. Både P1 og P2 brukte dette mønsteret. Under spørsmålene senere kommenterte P1 at mønsteret personen hadde brukt var veldig enkelt, og anså det som sannsynlig at andre ville kunne gjette seg frem til det. Personen mente i ettertid at det ville vært bedre å tegne et mer komplisert mønster siden det ville gjort det vanskeligere for andre å gjette seg frem til. P2 tegnet også samme mønster, og

kommenterte i ettertid at det selvfølgelig var mulig å tegne et mer komplisert mønster. Under vurderingen trakk også P4 frem den diagonale linjen som et enkelt mønster å tegne, men som ville blitt for enkelt for andre å gjette.

P3 hadde også noen vurderinger angående sikkerheten og kommenterte mekanismen kan være litt farlig siden det er lett å velge et symmetrisk mønster som andre kan gjette. Brukeren mente det var fort gjort å velge et mønster som er for enkelt, og personen tror de færreste vil velge et usymmetrisk mønster. Derfor foreslo P3 å gi brukere tips om mønstre. Derimot trodde P5 mekanismen var sikker, og lurte på om den kanskje er bedre enn vanlig kode.

5.9 Evaluering

Etter å ha forsøkt de forskjellige mekanismene, skulle brukerene vurdere dem opp mot hverandre, hva de likte og hvor sikre de trodde de var. Gjennom testene, var det en del brukere som hadde problemer med registreringen til de forskjellige mekanismene, men få som hadde problemer med innloggingen. Det var ingen som ikke logget seg vellykket inn med de tre forsøkene som var tilgjengelig for hver mekanisme. Det var også mulig å se hvordan brukerene ble mer kjent med systemet, og enkelte spørsmål som ble besvart for tidlige mekanismer ble ikke stilt på nytt selv om situasjonene kunne være rimelig like. Det virket også som brukerne hadde mindre problemer etter at de hadde vært gjennom registrering og innlogging med den første mekanismen, slik at de ble mer klar over hvordan testen var lagt opp.

5.9.1 Rangering

De forskjellige brukerene hadde ulike rangeringen av de forskjellige mekanismene, med forskjellige grunner.

P1 anså passord som greit, men synes bilde og lyd var veldig forvirrende, mens spørsmål og mønster var bra. Hovedproblemet med bilder og lyd var at det var ukjent, og veldig uklart hvordan brukeren skulle gå frem. Brukeren foretrakk mer kjente mekanismer som passord og spørsmål, men var også positivt innstilt til mønster.

P2 foretrakk passord og mønster, og var minst fornøyd med lyd og bilder. Passord var den foretrukne mekanismen siden personen var vant til denne mekanismen og mente den kanskje var tryggere. Personen likte lyd absolutt dårligst og fant den distraherende.

P3 vurderte spørsmål og passord som de beste mekanismene, lyd og mønster som de dårligste. Brukeren mente at konkrete, personlige spørsmål bør være lett å huske. Derimot synes personen bruken av lyd var naiv og

latterlig, men tror å bytte ut dyrelydene med andre lyder kunne hjulpet her. Brukeren hadde ikke lagt merke til at det var andre kategorier tilgjengelig i det hele tatt. Etter å ha blitt informert om dette, lurte brukeren på om det ville vært bedre å blande de forskjellige lydene.

P4 rangerte spørsmål og passord som de beste mekanismene, og mønster som den dårligste. Brukeren mente passord måtte være veldig bra, siden det er såpass utbredt som det er. Personen hadde stor tillit til mekanismen siden den blir brukt av banker, staten og mange andre tjenester. P4 trakk også frem at det var den eneste mekanismen fra undersøkelsen som er å finne i bruk. Personen likte også personlige spørsmål, og tror det er en mekanisme som kan passe godt for eldre.

P5 foretrakk visuelle mekanismer, særlig bilder og mønster, og mislikte lyd og passord. Personen likte spesielt de mekanismene som brukeren oppfattet som morsomme. P5 mente passord er litt meningsløst, og kommenterte det er irriterende å stadig måtte skrive inn passord for å logge seg inn forskjellige steder.

5.9.2 Grunnlag

Brukerne hadde ulike grunnlag for sine vurderinger. Sikkerhet var et punkt de fleste nevnte, selv om enkelte la mer vekt på det enn andre, av ulike grunner.

P1 sa personen ikke vurderte utifra tidsbruken under evalueringen av de forskjellige mekanismene, men heller la vekt på sikkerhet og gjenkjennelighet. P2 bedømte mekanismene utifra flere aspekter, men mente sikkerheten skilte passord og mønster. Brukeren mente passord var den beste mekanismen, sikkerhetsmessig. En litt annerledes vurdering kom fra P3, som ikke nødvendigvis var så redd for sikkerheten. Brukeren vurderte heller utifra hva som var lett å huske. P4 derimot, anså i utgangspunktet alle mekanismene som brukbare og rangerte mekanismene etter hvor sikre brukeren oppfattet dem. P5 la vekt på at det var personens egen subjektive evaluering av mekanismene og hva som var lett å huske. P5 la ikke mye vekt på sikkerhet, siden brukeren regnet med at den allerede er vurdert av andre og stoler på eksperter. Likedan sa også P1 at brukeren gikk ut ifra at de forskjellige mekanismene var like sikre.

5.9.3 Svakheter ved mekanismene

Brukerene ble både spurt hvordan de så på sikkerheten for de ulike mekanismene, og hvordan de så for seg uvedkommende kunne få tilgang ved bruk av dem. Også her hadde brukerene forskjellige vurderinger av hva de anså som sikkerhet, og hvilke trusler de så for seg. I stor grad så de for seg at angripere

ville forsøke å gjette seg frem til et passord eller hva brukeren oppga, men enkelte tenkte også på at angriperen kunne være noen som kjente offeret godt.

P1 vurderte sikkerheten på de ulike mekanismene utifra at andre kan jobbe seg frem til et passord, eller prøve seg frem til et mønster. Brukeren resonnerte seg også frem til at det kom an på hvem angriperen var. Hvis det var noen som kjente personen godt, ville det være enklere å gjette seg frem til svarene på de personlige spørsmålene.

P2 visste ikke ikke hva som er mest usikkert, men antok svarene til personlige spørsmål ville være lette å gjette seg til. Avanserte mønstre ville være vanskelig for andre å gjette seg til, men blir samtidig vanskeligere for brukeren å huske på. Brukeren så for seg at uvedkommende kunne prøve å gjette seg frem til mønster eller bilder, så det gjaldt å tenke ut noe komplisert som ikke kan gjettes av andre.

P3 mente lydene kan være lette å høre for andre, men brukeren mener også mekanismen kan være sikker hvis det forutsettes at lyden ikke høres av andre. Brukeren mente personlige spørsmål er sikrest, siden andre ikke kan vite eller gjette seg til svarene. P3 slo derfor fast at "[spørsmålene] MÅ være helt sikkert". Med mindre de samme spørsmålene også blir brukt andre steder, ser ikke P3 for seg at det er mulig for andre å gjette seg frem til svarene. På dette tidspunktet lurte personen på hvor svarene ble lagret og hvem som hadde tilgang til å se de.

Den største svakheten som P4 så for seg, var bruk av enkle mønstre til mønstergjenkjenningen. Personen antok folk ville lage enkle mønstre som er lette å gjette. Angripere som forsøker å få tilgang vil sannsynligvis prøve med de enkle mønstrene først. P4 så på de andre mekanismene som umulige å gjette seg til, men la til at det også er en fare for at andre kan overhøre lydene.

P5 tror personlige spørsmål er sikrest, siden utenforstående ikke vil kunne gjette seg til svarene. Brukeren mener at passord er letter å gjette seg frem til. Personen ser det som teoretisk mulig for andre å gjette seg frem hvis de har nøye kjennskap til brukeren. Brukeren trodde også det var en mulighet for gjette svarene på spørsmålene, men så ikke helt muligheten for de andre mekanismene. P5 la til at personen bruker huskeregler for passord, og mener det skal godt gjøres av andre å finne ut hvordan personen tenker.

5.9.4 Mulige problemer

For de ulike mekanismene la brukerene merke til mulige problemer, eller kommenterte aspekter de lurte på.

P3 mente mønstre kan bli vanskelig for andre å gjette seg frem til, men

samtidig vanskelig å huske for brukeren. Samme person tror et utvalg på 60 bilder til bildegjenkjenning kanskje er litt mye, og at antallet kan være vanskelige å huske hvis de ikke blir brukt daglig. P4 mente et stort antall bilder bør være sikkert, så lenge brukeren er i stand til å huske bildene sine.

Som beskrevet i detalj over, valgte mesteparten av brukerene heller enkle mønstre. P2 kommenterte at valg av avanserte mønstre kunne føre til problemer, og at det ble vanskeligere å huske. Personen mente at hvis et mønster ble brukt til f.eks. å logge på maskinen ville det gått greit, men med flere ville personen fått problemer med å huske de forskjellige mønstrene.

P5 så på seg selv som en visuell person, og likte mekanismene med bilder og mønstre. Personen mente det var en fare for å kunne glemme passord, men så ikke for seg å ha dette problemet med mønster eller bilder. Også personlige spørsmål var greiere sånn sett, med mindre sjanse for at svarene glemmes. Brukeren uttrykte også at mekanismene som bilder og mønster virket morsomme i bruk, og at personen likte dem.

Et flertall av brukerene mislikte lyder, og for P5 sin del mente personen at hovedproblemet med lyd var sammenhengen med bildet. Det var mer til hinder enn hjelp. Også andre brukere kommenterte at det var liten forskjell mellom lyd og bilder. P4 bemerket at lyder ikke vil fungere for tunghørte brukere.

6 Diskusjon

Med bakgrunn i både teori-kapitlet og funnene fra brukerundersøkelsen blir problemstillingen diskutert i denne delen. Først er det en kartlegging av ulike mekanismer som finnes med litt om hvor egnede de virker til bruk. Så følger en diskusjon rundt hvordan brukerne forholdt seg til mekanismene i brukertesten med problemer og områder som trenger forbedring. Til slutt forsøker vi å anslå hvordan brukernes mentale modeller overlappet med systemet, og hvilke trusler brukerne så mot de forskjellige mekanismene.

6.1 Hvilke ulike autentiseringsmekanismer er i bruk eller kan benyttes per i dag?

I litteraturen finner vi et bredt utvalg av forskjellige mekanismer som har blitt prøvd ut, tatt i bruk, eller forkastet av ulike grunner. Det er ikke hensikten her å dekke absolutt alle mekanismer som har blitt undersøkt, men heller velge ut og se på noen representative for ulike grupper mekanismer.

Samtidig har prototypen fokusert på mekanismer innenfor hva brukeren husker, slik at dette også blir hovedfokus her. Innlogging med mobiltelefon var en planlagt mekanisme for prototypen, men denne ble utsatt. Dermed vil denne delen i hovedsak dreie seg om mekanismene i prototypen og noen flere utover de, men mindre om mekanismer basert på hva brukeren har eller er.

6.1.1 Ulike nivåer og mekanismer

Alternative autentiseringsmekanismer kan være aktuelle i ulike situasjoner. Fornyings- og administrasjonsdepartementet har laget en forskrift [20] som angir fire ulike sikkerhetsnivåer for offentlige tjenester. De tar i hovedsak utgangspunkt i trusselnivået i forhold til hvor kritisk det er for tjenesten hvis andre skulle få tilgang.

De fire nivåene som har blitt angitt for ulike tjenester, innebærer hver ulik grad av sikkerhet i autentiseringen. Sikkerhetsnivå en har ingen spesielle krav, slik at mekanismer som selvvalgt passord og brukernavn eller kun identifisering med personnummer kan benyttes. Sikkerhetsnivå to krever mekanismer som fast passord eller passordkalkulator. Fortsatt holder det med autentisering med en faktor. Derimot krever sikkerhetsnivå tre autentisering med minimum to faktorer, hvor den ene skal være dynamisk. Eksempler på godkjente mekanismer er passordkalkulator beskyttet med PIN-kode eller engangspassord til mobiltelefon. Sikkerhetsnivå fire har like, men sterkere krav som nivå tre. I tillegg skal systemet kunne verifisere hvem som har utført handlinger i ettertid.

I tilfeller hvor tjenester har angitt ulike nivåer [20], vil det være mulig å benytte forskjellige mekanismer for å få tilgang til de ulike nivåene. Siden autoriseringen foregår etter at brukeren er autentisert, vil systemet kunne tildele rettigheter basert på mekanismen brukeren logget seg inn med. Vi kan tenke oss et system der brukeren har tilgang til å utføre vanlige oppgaver så lenge brukeren har autentisert seg, uavhengig av hvilken mekanisme som ble benyttet. Hvis brukeren derimot skal utføre mer administrative oppgaver, har systemet strengere krav for hvilke som mekanismer blir benyttet. Kanskje inkluderer kravene til og med autentisering med flere faktorer for at brukeren skal få tilgang. Hvis slike systemer benyttes vil det være fornuftig at de områdene av systemet som vil forårsake mest problemer eller størst skade for brukeren og systemet blir sikret. Men i tråd med tanker om hvordan brukere forsøker å finne snarveier i systemer [33] bør det også foretas en avveining i forhold til oppgaver brukeren vil gjøre oftere. Hvis det er noe brukeren gjør sjelden vil kanskje personen ha mindre imot å benytte ekstra tiltak som et smartkort eller kodegenerator, men hvis det er noe brukeren må gjøre ofte kan det tenkes brukeren vil gjøre prosessen enklere å utføre for seg, på kostnad av sikkerheten.

6.1.2 Problemet med passord

Passord blir brukt i omtrent alle datasystemer som håndterer innlogging, og er helt klart den mest kjente autentiseringsmekanismen. Mye av grunnen til at det er den mest utbredte løsningen, mener Sharma et al [44] kommer av at passord er en enkel, praktisk løsning med lave kostnader. Men selv om passord er mye brukt og de facto mekanisme for innlogging, er det likevel kjente svakheter ved mekanismen. Ved sin natur vil passord naturlig nok være vanskeligere å gjette for uvedkommende desto lengre og mer kompliserte de er. Dette gjør at brukere bør benytte lengre og mer kompliserte passord for å forsvare seg mot angripere som forsøker å gjette seg til passord. Men samtidig vil dette gjøre det vanskeligere å huske passordet, spesielt hvis det brukes sjeldent eller brukeren har mange andre passord å huske på.

I utgangspunktet var ikke dette et problem siden det var kun et mindre antall tjenester brukere var medlem av, men per i dag er de fleste medlem av en lang rekke forskjellige nettsteder og tjenester. Dermed ser vi blant annet at brukere tar i bruk teknikker eller egne verktøy for å huske passord [44]. En mulig taktikk er å bruke samme passord flere steder, men dette kan føre til at hvis uvedkommende avslører et passord får de samtidig adgang til andre steder. Det er også forskjellige systemer som baserer seg på å skrive ned, eller på annen måte lagre passordene på en trygg måte. Ulempen er selvfølgelig å sørge for at de ikke vil havne på avveie. Det er også et sosialt problem

ved at folk har generelt veldig lett for å gi fra seg passordene sine til andre hvis de tror de trenger tilgang. Utover de generelle problemene, rammer noen problemer spesifikke grupper, som f.eks. har dyslektikere vanskeligheter med å skrive lange passord.

Det har vært ulike forsøk for å få folk til å styrke passordene sine. Forget og Biddle [9] forsøkte å forbedre folks passord ved hjelp av interaktive systemer designet for å endre folks oppfatning og oppførsel. Et mulig forslag var å sette inn tilfeldige tegn når brukeren registrerte et nytt passord. Brukerene får dermed ikke valgt for enkle passord som er lette å gjette, uten at de blir for kompliserte til at det er mulig å huske. I Forget og Biddle [9] sitt eksperiment skulle brukere velge et passord først, som så fikk enten to tegn lagt til eller byttet ut for å gjøre det sikrere. Etterpå skulle brukeren skrive inn passordet igjen, og det ble målt hvor lang tid brukere brukte for å huske passordet. For brukere med lengre passord førte de ekstra tegnene til at de brukte lengre tid for å komme på passordet. Deltagere bemerket også at de ekstra tegnene skapte problemer for metodene de benyttet for å lage passord, og gjorde dem vanskeligere å huske. I tillegg gjorde de ekstra tegnene passordene for kompliserte for brukere som allerede var klare over farene og valgte sikre passord. De argumenterer derfor at det er viktig å ikke skyve ut brukere som er bevisste på sikkerhet og faktisk velger gode passord.

Selv om intensjonene var gode, kan det virke som de sikrere passordene skapte problemer for systemene brukere benytter for å huske passord, og ikke skilte ut passord som allerede var sikre nok. En mulig løsning er å avgjøre hvor komplisert passordet er før eventuelle tegn legges til eller endres. Siden målet er at passordet skal være så sikkert som mulig samtidig som det er enkelt å huske, bør det finnes klart definerte retningslinjer for hvor sterke passord som kreves. Hvis brukere er bevisste på sikkerhet og velger passord som er i henhold til kravene, burde de få lov til å velge de. Brukere som derimot velger svake passord, bør få tilbud om å legge til tegn som vil gjøre passordet sterkere, men fortsatt mulig å huske.

En mulighet for å håndtere en større mengde passord er ulike verktøy som kan lagre brukerens passordene. Slike verktøy kan sees på som nøkkelknipper og kan bla implementeres som et eget program som kjører i bakgrunn på maskinen. Ved behov for å logge seg inn, benytter brukeren programmet for å få tilgang til et spesifikt passord. De fleste verktøyene støtter et hovedpassord brukeren kan ha for å låse opp de andre passordene som har blitt lagret. Nøkkelknippene kan også inkluderes i andre programmer (de fleste moderne nettlesere innholder en), men det er også mulig å ha fysiske enheter brukeren kan ha med seg som f.eks. en USB-nøkkel. I en undersøkelse av Gaw et al [11] kom det frem at slike verktøy ikke var så populære, men de som oftest ble brukt er de innebygget i nettleseren fremfor dedikerte programmer.

Mesteparten av deltakerene i undersøkelse husket derimot passordene sine selv. De fant også at brukere benytter seg av nettsteder der de kan oppgi at de har glemt passordet sitt, slik at de får tilsendt et nytt. De benyttet seg også at nettsteder hvor det er mulig å hake av for å huskes ved senere anledninger. Det kommer ikke frem om brukerene gjorde dette for å unngå å huske passordet, eller om det var kun hvis de glemte det.

6.1.3 Passfraser

En annen mulig løsning for bedre passord, er å bruke flere ord eller setninger i en passfrase fremfor et passord [18]. En frase eller setning vil være lengre enn et passord, og vil dermed være vanskeligere å gjette seg frem til ved brute force eller finne i en ordliste. På samme måte som lengre passord kombinert med tall og spesialtegn er vanskeligere å gjette seg frem til, vil passfraser bestående av setninger gi mange muligheter som gjør det vanskeligere å gjette seg frem til. Angripere som bruker ordlister som inneholder vanlig ord og passord må utvide dem til å omfatte setninger for å kunne finne frem til alle, noe som vil kreve mye tid og arbeid. En ulempe med å benytte passfraser fremfor passord er nettopp lengden, som kan føre til at det blir vanskeligere for flere enn de som allerede har problemer med å huske passord. På den annen side kan det tenkes at kombinasjoner av flere ord gjør det lettere å huske enn med tall og spesialtegn som blir benyttet per idag. Et annet aspekt ved lengden er at det blir lettere å stave feil siden brukerne må skrive mer under innlogging.

Keith et al [18] gjennomførte en studie der de sammenlignet passfraser med passord med visse krav og passord brukerene fikk bestemme selv. 50 studenter var med i eksperimentet og fylte ut spørreskjemaet når studien ble avsluttet etter å ha vart i 10 uker. Ved registrering ble brukerne presentert en av tre mulige nettsider; en der de bare skulle oppgi et passord (kontrollgruppen), en der de skulle oppgi et passord som oppfylte visse krav (lengde, kombinasjon av store/små bokstaver osv.) og til slutt en der de skulle bruke en passfrase. For de to siste gruppene, ble de vist eksempler for å hjelpe deltagerene. I følge resultatene hadde kontrollgruppen de svakeste passordene, mens gruppene med passord med krav og passfraser hadde begge sterkere. Mye av styrken skyldes at de to gruppene hadde strengere krav på minimumslengde i forhold til kontrollgruppen.

De så derimot at gruppen med passfraser hadde den laveste suksessraten for innlogging. Keith et al [18] bemerker at systemet ikke oppgir grunnen til at innloggingen feilet, slik at det er vanskelig å avgjøre om det skyldes vanskeligheter med å huske passordet eller om det ble stavet feil. F.eks. der det skiller kun en bokstav fra det korrekte passordet, er det sannsynligvis

resultat av en stavefeil når brukeren skrev det inn, ikke et problem med å huske selve passordet. Etter å ha skilt ut en del innloggingsfeil som stavefeil, ble resultatene for vellykkete innlogginger mye jevnere. Sannsynligvis var de lengre passordene og passfrasene mer rammet av stavefeil fordi de var lengre. Men forskerne la også merke til at over tid gikk andelen feilstavelser ned for gruppen med passfraser.

Det kan tyde på at lengre passord, og passfraser har noe for seg, men det er mulig det går en viss periode der brukerne blir vant til å skrive de lengre passordene. Ved å legge til flere tegn, er det flere muligheter for å stave feil, og siden passord blir skjult er det ikke mulig å oppdage om deler er stavet feil før brukeren forsøker å logge inn. Samtidig er sannsynligvis denne mekanismen uegnet for brukere som har motoriske problemer og dermed får vanskeligheter med å skrive lengre tekster. For denne brukergruppen vil innloggingen ta mye lengre tid, i større grad enn den vil det for andre brukere, noe som kan være et poeng å ta med i vurderingen av alternative mekanismer.

6.1.4 Grafiske passord

Grafiske passord er en fellesbetegnelse for ulike løsninger der brukeren benytter seg av bilder, mønstre eller andre grafiske elementer fremfor å skrive et passord. Disse mekanismene være mer egnet for dyslektikere eller andre som har problemer med å huske ord. En av de lovende mekanismene er bildegjenkjenning der brukeren har valgt seg ut et sett med bilder som brukeren skal huske for å logge seg inn.

Sikkerhetsnivået for disse løsningene avhenger i stor grad av utvalget og antall bilder brukeren må identifisere. Antall bilder bør justeres med tanke på at et utvalg med for få bilder vil gjøre det enklere å gjette seg frem til brukerens bilder, mens et stort utvalg kan gjøre det uoversiktlig for brukeren under registreringen. I tillegg bør det vurderes hvilke symboler, ikoner, eller bilder som inkluderes i utvalget. Både for at bildene skal være unike nok til at brukerne kan skille dem, men også for å unngå bilder som større brukergrupper opplagt kommer til å velge. Under brukerundersøkelsen valgte flere av brukerne det norske flagget som et av bildene sine. Det er et naturlig valg, men kan tyde på at enkelte bilder bør sorteres ut hvis en stor andel av brukerene ender opp med det samme bildet. Hvis angripere legger merke til at det er en del bilder som kan være felles for et større antall brukere, kan de lettere gjette seg frem ved å forsøke disse bildene. Hvis de samme bildene blir brukt av flere brukere får angripere dermed lettere tilgang til en rekke forskjellige brukerkontoer.

Det er også et lite problem under innloggingen, som bør adresseres i en implementasjon. Ved innlogging blir brukeren vist en rekke bilder, hvor et av

dem er brukerens. Dvs. vil en angriper vite at minst et av bildene som blir vist er det riktige, og denne informasjonen kan utnyttes i en naiv implementasjon. Et enkelt angrep går ut på å forsøke å logge inn med et brukernavn angriperen har fått tak i og lagre de bildene som blir presentert. Siden angriperen ikke forsøker å gå videre eller logge seg inn, vil det sannsynligvis ikke telle som et innloggingsforsøk, dog avhenger dette av systemet. Hvis systemet henter ut et av brukerens bilder sammen med andre tilfeldige bilder, kan en angriper over tid kunne se mønstre i hvilke bilder som går igjen. Siden bildene brukeren logger seg inn med må være til stede, vil disse over tid bli vist oftere enn de tilfeldige som kan variere fra gang til gang.

I prototypen til brukertesten ble dette hullet tettet ved at brukerens bilder alltid blir vist med et fast utvalg andre bilder for en bruker. For hver bruker vil altså et riktig bilde vises under innlogging, samt et antall andre bilder som er fast og knyttet til det bildet for denne brukeren. En annen bruker som har valgt samme bilde vil ha et annet sett å gå ut i fra, så det ikke blir mulig å trekke konklusjoner for en bruker basert på andre. Dermed vil ikke angripere kunne analysere hvor ofte bildene opptrer siden de samme bildene blir vist sammen. Kombinert med et lavt antall forsøk før brukeren blir utestengt, setter dette en effektiv stopper for angrepsformen.

I et av forslagene som Suo et al [46], der det ble foreslått at bruker kunne laste opp egne bilder, og så under innlogging finne igjen sitt bilde blant en mengde andre bilder, eller ikke oppgi et bilde hvis bildet ikke var til stede. I utgangspunktet kan dette gjøre det lettere for brukeren å huske bildene sine. Men samtidig ser vi denne løsningen i stor grad avhenger av bildeutvalget. Angripere som analyserer innloggingen for en stor mengde brukere vil kunne peke ut hvilke bilder som er sjeldne eller går igjen oftere, og vil dermed kunne sirkle seg inn på brukerens bilder. Det kan også tenkes det er mulig å se forskjell i kvalitet eller motiv, eller hvis angriperen kjenner brukeren, kjenner igjen selve bildene som brukerens egne. I tillegg er det ulike aspekter ved åndsverksloven og personvern som kan spille inn på hvilke bilder en tjeneste kan benytte. Jeg tror derfor ikke det er en god ide å tillate brukere å laste opp egne bilder siden det kan gjøre det enklere for angripere.

Som Suo et al [46] foreslo, hadde prototypen innloggingen med bilder over flere ledd slik at brukeren måtte finne mer enn et bilde for å logge seg inn. Dette vil gjøre det vanskeligere for uvedkommende å gjette seg frem til brukerens bilder, siden de må gjette mer enn et. Samtidig gjør det at innlogging tar lengre tid. Dette virker derimot som en god sikring. Ved å kun velge et bilde, kan det være stor sjanse for at brukeren kan gjette seg til det, men det blir mer komplisert desto flere bilder som skal gjettes. Systemet bør heller ikke gi tilbakemelding i form av hvor mange bilder som var riktige, men heller gi beskjed om at et eller flere var feil ved mislykket innlogging, slik som

i prototypen. Dette gjør at angripere ikke vil vite om de har funnet frem til noen riktige bilder, eller om alle var feil, som er informasjon angripere ikke bør ha tilgang til. Kombinert med et antall forsøk før brukeren blir utestengt, anser jeg dette som en god sikring av mekanismen.

Både for bilder og mønstre er et problem at andre som ser over skulderen til brukeren vil se hva brukeren logger seg inn med. I litteratturen blir det diskutert få mottiltak, men Gao et al [10] har et forslag der brukeren trekker linjer fra et punkt til et annet som er innom alle bildene til brukeren og eventuelle andre. Men samtidig var det mulig for andre å se hvor brukere stoppet opp og lette etter neste bilde, så det er mulig dette forslaget ikke løser problemet helt. Da virker det heller som om det heller kan gi brukere falsk trygghet, ved at de tror andre ikke kan se hva de velger, selv om andre kan se hvor de stopper underveis. En alternativ fremgangsmåte er å instruere brukerne i å kun logge seg inn når de er alene, men det er ofte ikke gjennomførbart og det virker også feil å skyve hele ansvaret for sikkerheten over på brukerens side. Det er med andre ord flere lovende mekanismer som tar i bruk grafiske passord, men de kritiske elementene er å sikre et godt utvalg muligheter og at det ikke blir vanskelig for angripere å gjette seg frem til hva brukeren har valgt. Til slutt er det fortsatt et problem med at andre kan se hva brukeren velger, hvor den beste løsningen hittil sannsynligvis å være oppmerksom på om noen følger med på innloggingen.

6.1.5 Lyder

Spesielt for blinde eller svaksynte brukere, har ulike mekanismer basert på å huske et sett lyder blitt foreslått. I prototypen inkluderte mekanismen med lyd også bilde og forskjellige kategorier, men det har også vært forslag der kun tekst og lyd blir benyttet. Den åpenbare trusselen er at andre i nærheten skal høre brukerens lyder, men en løsning er å bruke hodetelefoner under innloggingen. Brukeren vil fortsatt kunne høre lydene som spilles av, men det blir vanskelig for noen i bakgrunnen å overhøre dem.

Enkelte sider og tjenester per idag er nærmest umulige å bruke siden de fungerer dårlig med skjermlesere eller andre hjelpemidler. Et av de større problemene er CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart). CAPTCHAer består ofte av bilder med tekst som skal skrives av for å bevise for et nettsted av brukeren er en person, ofte som en del av registrering. Dette gjør det meget vanskelig for blinde og svaksynte siden de er avhengig av å kunne identifisere hva de skal skrive av avbildningen. Noen CAPTCHAer har forsøkt å løse dette problemet ved å tilby en kort snutt som leser opp tegnene som er avbildet, slik at brukerene vil kunne skrive av denne istedenfor.

Lyder kan være en lovende mekanisme som i større grad lar brukere og svaksynte brukere logge inn. Det er uvisst i hvor stor grad mekanismen vil være aktuell for andre brukere, men kan likevel sees på som en mulighet. Enkelte av brukerne i testen lurte på hvordan det gikk hvis brukeren trengte høreapparat eller var tunghørt. I slike tilfeller er sannsynligvis ikke denne mekanismen den best egnede, og en alternativ bør benyttes i stedet. Likevel tror jeg innlogging med lyd kan bidra som et del av et spekter for ulike mekanismer, og kanskje legge bedre til rette for blinde og svaksynte brukere.

6.1.6 Personlige spørsmål og svar

Brukere kan autentisere seg ved å svare på et sett personlige spørsmål. Også her er det nyttig å bruke mer enn et spørsmål under innloggingen slik at andre ikke kan gjette seg frem til svarene. Ved å ha flere ledd å forholde seg til, må de gjette svaret på alle for å logge inn. Den største faren er at angriperen er noen som kjenner brukeren godt eller kan finne frem informasjonen til å svare på spørsmålene, som enkelte nevnte under brukertesten.

Spørsmål og svar er delvis i bruk, og benyttes av forskjellige tjenester hvis brukeren glemmer passordet sitt. Ved å svare på spørsmål knyttet til profilen eller informasjon brukeren oppga ved registrering beviser brukeren for nettstedet at personen er den rettmessige brukeren. Dermed kan brukeren få tilgang til kontoen sin eller tilbakestilt passordet.

En av fordelene med personlige spørsmål kontra passord, som ofte er noe brukere må lage nye fra tid til annen og finne på nye systemer, kan spørsmålene baseres på noe brukeren har visst lenge. Ved å utnytte eksisterende kunnskap kan brukeren slippe prosessen med å pugge og lære seg et nytt passord, men heller knytte noe personen allerede vet til tjenesten. Som en person kommenterte under brukertesten, er det ikke nødvendig å aktivt huske på f.eks. hva moren din heter. På den måten får mekanismen mye sikkerhet gratis, ved at brukeren kan velge mer avanserte ting som brukeren allerede husker. Jeg synes det virker som en god ide å utnytte hva brukeren allerede har lært seg og kan, fremfor å kreve at brukeren skal bruke mye energi på å lære seg et nytt passord. Brukere er generelt mer opptatt av å utføre det de skal enn å fokusere på sikkerheten [33], så det er mulig spørsmålene kan legge bedre til rette for at brukerne kan raskere gå videre med hva de vil samtidig som sikkerheten fortsatt ivaretas.

En mulig ulempe er at brukerne i stor grad står fritt til å velge sine egne spørsmål, som innebærer de kan velge seg enkle spørsmål som andre lett kan finne ut svarene til. I brukertesten nevnte noen at personer som kjente brukeren godt kunne finne svarene på spørsmålene, mens andre var sikre på at andre ikke ville kunne gjette seg frem til svarene. En bruker foreslå også

å gi brukerne hjelp slik at de ikke skulle velge for enkle spørsmål.

Jeg tror spørsmål kan være en god mekanisme som gjør at brukere kan velge mer kompliserte svar som de likevel husker selv, men som andre ikke vil vite. Det er bare fantasien som setter grenser for hvilke spørsmål brukerne kan hente frem som andre ikke vil vite svaret på. Vanskelighetsgraden til spørsmålene er likevel det viktigste punktet, og hvis brukeren velger enkle spørsmål som andre vet eller lett kan finne svaret på hjelper ikke mekanismen så mye.

6.1.7 Kodegeneratorer

Kodegeneratorer blir spesielt brukt i sammenheng med nettbank. De baserer seg på noe brukeren har, og generatoren brukes til å få en engangskode brukeren skal oppgi som en del av autentiseringen. De kan brukes alene, men egner seg også som en del av autentisering med flere faktorer. Gitt at engangskodene er tilfeldige, og andre ikke vil kunne forutse dem, vil mekanismen være både egnet og sikker for viktige transaksjoner. Hvis brukeren passer godt på generatoren sin, eller den er kombinert med en annen mekanisme, f.eks. et passord eller noe annet brukeren skal huske, er den sannsynligvis sikker.

Selve kodegeneratoren virker sikker nok til at et annet element blir det svakeste ledd i denne sammenhengen. Siden koden kun kan brukes en gang, setter det en umiddelbar stopper for gjenbruksangrep. For denne mekanismen blir kommunikasjonen med tjeneste viktigere, for å unngå mann-i-midten angrep eller andre måter angripere kan utgi seg for eller endre hva brukeren gjør.

Både noe brukeren har og hva brukeren her (se nedenfor) brukes ofte i kombinasjon med noe brukeren vet. Ved å ta utgangspunkt i et passord eller lignende mekanisme kan gjenstander eller biometri forsterke sikkerheten, siden det blir vanskeligere for mulige angripere å få tak i begge deler. Som angitt [20] vil tjenster kreve ulike nivåer av sikkerhet, som vil si at forskjellige ting brukere husker kan kombineres med gjenstander eller biometri. Dette gjør det mer mulig å bytte ut passord-delen med alternative mekanismer. Det er f.eks. mulig å tenke seg bildegjenkjenning eller tegning av mønster i kombinasjon med en kodegenerator som vil kunne tilby samme sikkerhetsnivå som det ville gjort med passord. Så lenge hver enkelt mekanisme er sikker nok for seg, vil den økte sikkerheten av kombinasjonen bane vei for mulige kombinasjoner. Dette gir flere muligheter som kan både gjøre det vanskeligere for angripere å finne ut hvilken kombinasjon brukeren har valgt, men kan også gjøre det enklere for brukeren å huske sin innlogging.

6.1.8 Biometriske mekanismer

Ulike mekanismer baserer seg på biometriske data. Her er et av de kritiske kravene at mekanismene er i stand til å skille mellom brukerne. Siden de fleste mekanismene fortsatt er under utvikling er det enkelte av dem som er unøyaktige. Mekanismer for stemmegjenkjenning kan nekte brukere adgang hvis de er forkjølet en dag, eller fingeravtrykkskannere som gir uvedkommende tilgang fordi kontrollen er for dårlig er to av eksemplene. Selv om mekanismene er under utvikling, og sannsynligvis vil forbedres med tiden, er det sannsynligvis klokt å ikke bruke biometriske mekanismer unna kritiske systemer, eller kun bruke de i kombinasjoner med andre mekanismer. En annen grunn til å holde biometriske mekanismer unna kritiske systemer er å unngå å gi angripere insentiv til å kutte av brukeres kroppsdeler for å få tilgang. F.eks. fingeravtrykklesere som ikke registrerer kroppsvarme vil kunne akseptere avkappede lemmer, noe som potensielt setter brukerne i fare. Men hvis belønningen for tilgangen er liten, øker terskelen for å kutte av kroppsdeler og faren er sannsynligvis unngått.

Mekanismer som signatur eller håndskrift kan være lovende og vil være enkle for brukere å huske. En mulig fare er at signaturer har tidligere blitt brukt utenfor digitale sammenhenger og har blitt forfalsket på ulike vis opp igjennom historien. Daler et al [5] mener likevel at så lenge bevegelse og trykk registreres vil mekanismen være god nok. Sannsynligvis kan disse detaljene være med på å gjøre mekanismen sikker nok slik at uvedkommende ikke kan forfalske underskriften.

Hvis biometri skal tas i bruk i større grad, bør det også være alment tilgjengelig. Flere mekanismer baserer seg på skanning av kroppsdeler som for et fåtall ikke er mulig, eller bevegelser som er vanskelige for enkelte å gjennomføre. Maple og Norrington [24] foreslår at skannere bør plasseres tilgjengelig for personer i rullestol eller med andre utfordringer i forhold til å komme seg til der skanneren er, slik at de kan bli autentisert. Vi bør også vurdere å justere teknologien som blir benyttet i forhold til brukerene, fremfor å trene opp brukerene til å bruke teknologien. Jeg tror det er viktig at mekanismene legger til rette slik at flest mulig kan bruke dem, men at de som bruker slike mekanismer også har et alternativ for brukere som av ulike grunner ikke kan benytte dem. Selv om brukere som f.eks. ikke kan bruke fingeravtrykk fordi de mangler fingre er en minoritet, er det likevel viktig at det finnes alternativer, slik at også disse brukerne ikke blir sperret ute av mekanismene.

Potensialet til biometriske mekanismer er stort, siden det vil kunne basere seg på noe brukere alltid har med seg. Det er i liten grad mulig å glemme eller miste kroppsdeler, selv om sistnevnte skjer og bør tas høyde for. De er

ulike mekanismer basert på gangelag eller bevegelsesmønstre som kan være aktuelle, men felles for de fleste er at de ennå er under utvikling og bør studeres nøyere før de blir tatt i bruk. Gitt at utviklingen leder til mer nøyaktige mekanismer tror jeg biometri har et stort potensiale, så lenge det fortsatt tilbys andre mekanismer til brukere som ikke kan (eller vil) bruke dem.

6.1.9 Single sign-on

Single sign-on gjør at brukere kan få tilgang til flere tjenester eller ressurser ved hjelp av den samme påloggingen. Et slikt system kan være fordelaktig for enkelte situasjoner, f.eks. ved en arbeidsplass eller i en organisasjon. Her vil det være lett å se hvordan de ulike tjenestene kan knyttes sammen slik at den samme innloggingsinformasjonen gir tilgang til ulike deler innenfor den samme organisasjonen. SSO kan derimot virke mer komplisert, hvis brukerene blir presentert for tilsynelatende uavhengige tjenester eller ressurser der den samme innloggingsinformasjon kan benyttes.

SSO er en lovende mekanisme som kan bidra til å redusere noe av kompleksiteten ved autentisering ved at brukere i større grad kan forholde seg til en innlogging. På den annen side er det viktig for brukerne å kunne vurdere hvor de vil trekke grensen og hvilke tjenester de vil knytte sammen. Selv om det blir enklere ved å forholde seg til en innlogging, blir det desto mer kritisk hvis uvedkommende får tilgang og kan misbruke en større rekke tjenester. Derfor bør det kanskje vurderes å samle tjenester som hører naturlig sammen, men være kritiske til å kombinere alle tjenester for å unngå å legge alle eggene i en kurv.

Sett på en måte er SSO uavhengige av de andre autentiseringsmekanismene, og kan forsåvidt kombineres med forskjellige. Hovedoppgaven til SSO er å knytte forskjellige tjenester eller systemer sammen slik at autentisering et sted også kan benyttes andre steder. Hvilke mekanisme som benyttes til det er mer en detalj, og legger opp til spennende muligheter for bruk av alternative mekanismer. Det gjør det mulig for brukere å selv velge mekanismene de bruker som fortsatt gir tilgang til tjenestene de bruker.

6.1.10 Globale innstillinger

En liten digresjon, men fortsatt et aspekt som spiller inn på autentiseringen uavhengig av hvilke mekanisme som er valgt er de globale innstillingene for innlogging. Hvis en angriper har fått tak i et brukernavn, hjelper det lite hvilken mekanisme som har blitt benyttet hvis angriperen kan få tilgang gjennom et automatisk angrep som forsøker alle muligheter. Denne mulighe-

ten minker drastisk, hvis det kun tillates et mindre antall innloggingsforsøk for en bruker før kontoen blir sperret. Blant de globale innstillingene som kan benyttes for en løsning er å sette antall innloggingsforsøk som tillates, hvor lenge brukeren blir suspendert etter antall mislykkede innlogginger og antall suspenderinger som tillates før kontoen stenges.

I prototypen hadde brukerene tre forsøk på å logge seg inn, og selv om flertallet klarte seg på første forsøk hadde enkelte behov for et andre forsøk for enkelte mekanismer. Men samtlige brukere klarte seg innenfor de tre forsøkene de hadde tilgjengelige. En angriper som forsøker å gjette seg frem vil sannsynligvis ikke komme langt på tre forsøk. Ved å tillate flere forsøk gir det mulighet for legetime brukere å rette opp hvis de har skrevet eller valgt noe feil, eller har vanskeligheter for å huske passord eller lignende. For uvedkommende derimot som ønsker å prøve en lang rekke passord i tilfelle noen av dem gir tilgang, blir de stengt ute tidlig i prosessen, sannsynligvis før de har mulighet til å gjennomføre et effektivt angrep. Gjentatte feil ved innlogging kan tyde på at noen andre enn brukeren forsøker å få tilgang, og brukerkontoen bør suspenderes for en periode eller i verste fall stenges. For å unngå at den rettmessige brukeren sperres ute, bør sperren være midlertidig, og hvis problemet gjentar seg bør også brukeren kontaktes for å gjøres oppmerksom på problemet. I slike tilfeller bør brukeren få klar tilbakemelding på hva som skjer, slik at personen eventuelt kan ta sine forhåndsregler.

6.2 Hvordan fungerer et utvalg av av disse mekanismene under utprøving med brukere i praksis?

På grunnlag av resultatene fra brukerundersøkelsen er det mulig å si noe om hvordan brukere opplever de forskjellige mekanismene i praksis. Siden brukerne i undersøkelsen alle var seniorbrukere, er det vanskelige å si om resultatene gjelder generelt for hele befolkningen. Det er likevel enkelte aspekter som peker seg ut og elementer som var mulig å se for flere av testpersonene som kan gi indikasjoner på problemområder eller hva brukere foretrekker. Ofte er det et stort spenn mellom hva som forventes av mekanismene i forhold til hva som er forventede problemer og hva som i realiteten er problematisk. Fokus bør være på hvilke utfordringer brukerne faktisk opplever og ta hensyn til disse, slik at de i størst mulig grad fortsatt kan benytte tjenesten.

En klar svakhet med undersøkelsen er at brukerne forsøkte å logge seg inn direkte etter at de hadde registrert seg. Det ble ikke følgt opp eller kontrollert senere hvordan de forholdt seg til mekanismene over tid. Andre undersøkelser har sett på hvordan brukere er i stand til å huske passord, eller andre mekanismer over lengre tid, men det ble ikke gjort her. For å få et mer helhetlig

bilde av de forskjellige mekanismene kunne det vært interessant å se hvor mange av brukerene som fortsatt husket hva de hadde registrert og kunne logge seg inn etter f.eks. en uke, men det ble av ulike grunner ikke gjort i denne undersøkelsen. Det er derimot mer fokus på det umiddelbare inntrykket brukerene sitter igjen med etter å ha forsøkt de forskjellige mekanismene.

En fare som alltid er til steder når brukere studeres under undersøkelser er Hawthorne-effekten, dvs. at personene som blir observert gjør det bedre fordi de vet de blir observert enn de ville gjort hvis de ikke ble observert. Deltagerne var også forholdsvis erfarne brukere, og det er uvisst om nybegynnere ville forholdt seg til mekanismene på samme måte.

6.2.1 Valg av mekanismer

For å kunne velge autentiseringsmekanisme(r) for en tjeneste er det viktig å se på hvilke behov og utfordringer brukeren har. Et av målene med å se på alternative mekanismer er for å finne ut hvem som kan brukes til forskjellige tjenester. Enten for å tilby andre mekanismer generelt, eller for å dele inn tjenester i kritiske og mindre kritiske delere, der de mindre kritiske har færre krav til sikkerhet og andre mekanismer kan brukes. Det er ikke nødvendigvis slik at alle steder som krever innlogging er avhengig av høyeste sikkerhetsnivå. Det kan i tilfeller være sikrere å tillate en alternativ mekanisme enn en som brukeren vil gå rundt. Hvis brukeren benytter seg av snarveier som å skrive ned passordet, hjelper det lite hvor sikker tjenesten er tiltenkt å være, siden brukeren svekker den. Derimot, hvis andre mekanismer benyttes som brukeren er mer komfortabel med, er det sannsynlig brukeren kan være med og opprettholde sikkerheten i større grad. Men for å vite hvilke som kan benyttes, er det viktig å vite hvilke brukerne faktisk foretrekker.

6.2.2 Generelt

Et par generelle observasjoner gjelder for flere av mekanismene. Enkelte av brukerne hadde problemer i registreringsfasen, men det var kun et fåtall som hadde problemer med innlogging. De få som var ble i stor grad løst av brukerne selv, og det var ingen som ikke klarte å logge seg inn på de tre forsøkene som var tilgjengelige. Det kan tyde på at etter at brukerne har blitt vant med mekanismene gjennom registrering forstår de for det meste hva de skal gjøre.

For mekanismer hvor det var aktuelt ble det vist et område nederst på skjermen med det aktuelle utvalget, f.eks. for lyd og bilder. Ved å klikke på hva brukeren hadde valgt her, kunne brukeren velge det bort igjen. Teksten som ble vist over dette området kunne under piloten oppfattes som en ordre,

men ble senere justert til å bedre signalisere at det var en mulighet hvis brukeren angret og ville bytte ut et av bildene eller lydene. Etter endringene så det ikke ut til at andre brukere hadde problemer med denne delen, men det så heller ikke ut til at den ble brukt, så det er fortsatt mulig den ikke er klar nok. Det er også mulig den er overflødig og at brukerene så lite behov for å endre bildene de hadde valgt. Det var også mulig å velge bort igjen bilder eller lyd ved å klikke en gang til, så det er mulig visningen nederst kunne vært sløyfet.

Generelt sett var lyd var den desidert dårligst likte mekanismen, mange mislikte også bilder, mens passord og personlige spørsmål i stor grad var godt likt. Meningene var veldig delt om mønster, det var noen som likte den, mens andre som ikke likte den i det hele tatt. Det er uvisst i hvor stor grad standardvalget for lyd påvirket synet på mekanismen, men det var også brukere som sa de ikke så poenget med å bruke lyd i det hele tatt. Bakgrunnene for vurderingene var også delte. Mens enkelte av brukerene tok med sikkerhet i vurderingen, la andre mer vekt på at det var noe som var lett å huske, eller regnet med at andre allerede hadde avgjort om mekanismene var sikre nok.

6.2.3 Passord

Passord er sannsynligvis den mest utbredte mekanismen for autentisering, og flere av brukerene kommenterte at de var kjent med passord fra tidligere. Mange hadde ulike systemet for passord basert på navn og årstall eller datoer, som de regnet med de ville huske. Enkelte brukere bemerket også at de skrev ned passordene sine. En bruker var klar over at dette ikke egentlig var sikkert, men ønsket likevel å ha dem nedskrevet i tilfelle personen skulle glemme dem. Det er ikke mulig å vite om systemene brukerne hadde laget seg er vanskelige eller enkle å gjette seg frem til for utenforstående. Men det viser likevel at brukeren har tatt innover seg hvordan passord fungerer, og selv laget egne systemer de forholder seg til. Brukeren som var klar over at passord ikke burde skrives ned ser også ut til å være klar over konsekvensene for sikkerheten, men ønsker å ha en sikkerhetskopi av passordene sine.

Kombinasjonen av bokstaver og tall var kjent, men enkelte bemerket at de ikke var vant med å kombinere store og små bokstaver. Målet med å kombinere forskjellige tegn er for å gi uvedkommende et større spekter de må gjette fra. Både de potensielle mulighetene av tegn passordet består av såvel som lengden på passordet vil gjøre det vanskeligere for uvedkommende å finne frem til. Etter å ha registrert passordet, telte en av brukerene antall tegn, for å forsikre seg om at det var like langt som minimum. Både for passord og mønster brukte brukerne i stor grad minimumskravet på lengde

av passord/mønsteret. Samme bruker var selv i stand til å korrigere passordet etter at brukeren fikk tilbakemelding på at det ikke inneholdt nok tall. Det kan tenkes brukerne regner med minstekravet er sikkert nok, og ikke ser behovet for ytterligere tegn. Det forutsetter at kravene som har blitt satt fra systemet er gode nok til at brukerne har gode passord. Det er ikke sikkert brukerne holder seg til minimumskrav også utenfor testen, men det kan være sannsynlig.

Som mekanisme var passord middels likt, og alle unntatt en av brukerene logget inn på første forsøk. Den sistnevnte brukeren logget seg derimot fint inn på andre forsøk etter å ha skrevet passordet på nytt. Det så ikke ut til at noen av brukerne hadde noen særlige problemer med mekanismen, men den er kjent så det er sannsynlig brukerne visste hvordan passord fungerte på forhånd.

En av brukerene kommenterte at personen var lei av å stadig skrive inn passordet sitt på nettsteder for å logge inn. Det vil variere ettersom hvor mange sider brukeren er medlem av, men i stor grad er det flere sosiale nettsteder og tjenster som det er mulig å være medlem av en tidligere, noe som gjør at det blir mer å holde orden på. Brukeren som var lei av passord, var derimot positivt innstilt til mer visuelle mekanismer, som kan tyde på at alternative mekanismer kan hjelpe på situasjonen. Enkelte brukere kommenterte også underveis at de foretrakk bilder eller personlige spørsmål. At brukere blir lei av å stadig oppgi passordet sitt kan tyde på at de ser på sikkerheten som en kneik i veien for det de skal gjøre. Sannsynligvis vil brukere med denne innstillingen benytte seg av de muligheter de finner som kan gjøre at de slipper å forholde seg til passordet, som gjør det enklere å få gjort det de skal. Dessverre kan dette gå på bekostning av sikkerheten.

6.2.4 Bildegjenkjenning

Bortsett fra noen problemer under pilottesten med hvordan bilder skulle velges, forstod de fleste brukerne hvordan bilder skulle velges og hvordan de tok i bruk mekanismen. Etter at instruksjonene ble gjort klarer, virket det ikke som om de andre brukerene hadde problemer med å velge bilder. Selv om en av brukerne kommenterte at personen ikke likte det, var det heller ingen som hadde problemer med å måtte bla opp og ned på siden. Siden en bruker ikke likte det og det kan tenkes andre brukere får problemer med å bla, bør kanskje designet av denne delen revurderes. Under innlogging lurte en av brukerne først på om flere bilder brukeren hadde valgt ble vist på en gang, men oppdaget ved å se nærmere at kun et av bildene var der. Det virket som de fleste brukerne forstod mekanismen godt, og ikke hadde problemer med bruken.

De fleste brukerne studerte de forskjellige bildene mens de valgt sine. Enkelte mente i ettertid at utvalget kunne bli litt overveldende, mens andre bemerket at det var nødvendig med et større antall bilder for at mekanismen skulle være sikker. Andre igjen mente at utvalget kunne være stort, men det ville hjelpe hvis det var noe som ble brukt ofte slik at det blir mindre vanskelig å huske. Selv om enkelte kommenterte at det var veldig stort utvalg så det ikke ut som om noen av testpersonene hadde problemer med å velge bilder eller bla gjennom utvalget.

Et problem pekte seg ut med bilder, var det norske flagget som gikk igjen i utvalget til flere brukere. Et naturlig valg, men kan tyde på at enkelte bilder bør sorteres ut for unngå at en stor andel av brukerne ender opp med det samme bildet. Dette ble diskutert litt på forhånd i prosjektet, og det var forventet at en del ville benytte seg av det. Sikkerhetsmessig kan slike bilder gjøre det lettere for angripere å gjette seg frem til hvilke bilder brukeren har valgt. Hvis det er nok bilder som går igjen ofte, får angripere et godt utgangspunkt til å gjette seg frem, og kan få tilgang til flere brukere basert på hva som velges ofte. Derfor er det bedre å eliminere slike bilder så brukerne får mer unike utvalg som gjør det vanskeligere for angripere å gjette seg frem til bildene. Angriperen som kjenner en spesifikk bruker og vil ha kjennskap til hvilke bilder den personen velger er ikke en del av denne vurderingen. Dette er hovedsaklig for at angripere ikke skal kunne gå utifra hvilke bilder større brukergrupper velger seg.

Et annet problem med grafiske passord er andre som ser over skulderen vil legge merke til hvilke bilder brukeren velger. Prototypen hadde ingen mekanismer for å bøte på dette, og det var heller ingen brukere som nevnte det som en potensiell trussel. Det er usikkert om det var fordi de ikke så det som en trussel, eller om de ville passet ekstra på hvis de skulle logge inn med ukjente til stede.

Til tross for få problemer, og de fleste så ut til å finne fem bilder hver uten problemer, var det få som likte mekanismen godt. En av personene hadde derimot tro på mekanismen og mente den kunne være noe for eldre, kanskje for folk generelt.

6.2.5 Gjenkjenning av lyder

Det er tydelig at lyder var problematisk. Bortsett fra piloten, fikk ingen av brukerene med seg de forskjellige kategoriene eller forstod hvordan de skulle bytte kategori. Selv om en av brukerene siterte instruksjonene der det var oppfordret til å velge lyder fra flere kategorier, og en annen i ettertid lurte på hva bildene på venstresiden gjorde. På forhånd ble de diskutert i forskningsprosjektet om bilder og lyd skulle deles opp i kategorier eller

vise alle valgmulighetene samlet. I utgangspunktet ble både bilder og lyder delt inn i kategorier, men etter problemene under pilottesten ble alle bildene samlet. Samtidig ble inndeling beholdt for lyder for å se om det var noen forskjell mellom de to mulighetene. Det ser ut som at et samlet utvalget er den foretrukne måten.

På venstresiden ble det vist forskjellige bilder for å representere de ulike kategoriene, og den gjeldende var merket med en annen bakgrunnsfarge. Det kan virke som om dette ikke var nok, og hvis kategorier bør andre teknikker benyttes for å gi brukeren bedre tilbakemelding om hvilken kategori brukeren befinner seg i og de valgmuligheter som finnes. Den enkleste måten å løse dette problemet ville være å slå sammen alle kategoriene på lik linje med hva som ble gjort med bilder. Til tross for at brukerne var nødt til å bla for å kunne se hele utvalget, så det ikke ut til at noen av brukerene hadde noen særlige problemer. En annen løsning ville være å forsterke informasjonen rundt kategoriene, ved å legge til tekst. Per i dag ble kun bilder benyttet for å representere de ulike lydkategoriene. Ved å legge til tekst under hvert bilde, f.eks. "dyrelyder", "musikk" osv. kan det kanskje bidra til at brukere legger bedre merke til og forstår hva bildene på siden er til. En av brukerene lurte i ettertid på hva de var til, men visste ikke at de var for å bytte kategori. Samtidig kan det tenkes at en kort tekst over de forskjellige kategoriene i form av en oppfordring til å kunne bytte kategori eller tilbakemelding for hvilken kategori som blir vist nå, egner seg bedre for å vise at det finnes flere muligheter og lyder brukeren kan benytte seg av.

Selv om de ikke ble brukt, ble en av kategoriene byttet ut etter pilottesten. Musikk fra filmer ble fjernet siden piloten ikke kjente til noen av lydene der, og det var tvil om de andre brukerne kjente til filmene. Filmer ble byttet ut med musikkinstrumenter, og det ble antatt flere ville ha et forhold til dem. Sanger inneholdt også et utvalg av eldre, etablerte artister slik at det er trolig de fleste har hørt sangene før og har et forhold til dem. Siden kategoriene ikke ble brukt senere, er det uvisst hvor bra de egnet seg.

Det var også et par uklarheter ved innlogging. En av brukerene klikket på andre lyder enn det personen hadde valgt under innloggingen og henviste til teksten som sa "trykk på en lyd". Personen hadde forstått at det var sine egne lyder som skulle velges, men ville fremheve hvordan andre kunne misforstå teksten. Denne teksten bør sannsynligvis endres slik at det kommer tydeligere frem at det er brukerens lyder som skal velges. En annen av personene så ut til å tilsynelatende fortsette å velge lyder blant de tilgjengelige ved innloggingen. Brukeren forsøkte å velge nye lyder, men ble minnet på at kun en skulle velges under innlogging når brukeren spurte hvorfor kun en lyd var merket etter å ha klikket på flere.

Lyder var dårlig likt av de fleste brukerene, og en del kommenterte også

at sammenhengen med bildet var rart. Noen mente mekanismen ble veldig lik bilder, uten at selve lyden tilførte så mye. En av brukerne mente det var en barnslig mekanisme mens andre ikke så poenget med den. Det er uvisst om dyrelyder, som var standardvalget kan ha påvirket denne oppfatningen og at en kombinasjon eller valg av en annen kategori kunne ha gitt et annet bilde av mekanismen. Allikevel er det interessant å se hvordan en mekanisme som var meget lik bilder ble oppfattet såpass mye dårligere. Hvis denne mekanismen skal benyttes videre bør den sannsynligvis endres og legge bedre til rette for at brukere skal være klar over det totale utvalget enn hvordan mekanismen er utformet per idag.

6.2.6 Personlige spørsmål og svar

Ved bruk av spørsmål var det både brukere som laget egne spørsmål, og de som ikke så behovet. Hver av gruppene var omtrent halvparten av brukerene. Et større utvalg tilgjengelige spørsmål kunne kanskje gjøre at færre brukere så behovet for å lage egne spørsmål, men det kan fort bli uoversiktlig og forvirrende med mange spørsmål. En annen ting å legge merke til var at alle brukerene benyttet seg av noen av de tilgjengelige spørsmålene, så selv de som la til egne spørsmål fant noen de likte blant dem. Sannsynligvis er det bedre å ha et utvalg gode spørsmål som fleste av brukerne kan relatere til, og ha muligheten for å legge til egne for de som ikke finner passende spørsmål, eller av andre grunner ønsker å bruke egne.

Enkelte personer brukte lang tid på å tenke ut og legge til egne spørsmål, noe som kan være et tegn på at brukerene forsøkte å komme på noe de ville huske, men som andre ikke ville vite. Samtidig er det vanskelig å komme på et større antall spørsmål slik på stående fot. Det er uvisst om enkelte brukere ville ha gitt opp fordi det tok for lang tid, eller om de hadde benyttet enklere spørsmål.

To av brukerene kommenterte at spørsmålet om hva bestefaren din het, ikke er klart nok siden alle har to bestefedre. En av brukerne valgte til og med å legge inn et hint for hvilken side av familien bestefaren var fra. Det er mulige slike spørsmål bør bli gått gjennom før de blir benyttet i en virkelig tjeneste for å unngå tvetydige eller uklare spørsmål. Målet med spørsmålet var sannsynligvis at brukerne selv kunne velge, men som det kom frem, kan det være vanskelig å huske i ettertid.

En av brukerne begynte å legge til egne spørsmål etter å ha valgt fem av de som var oppgitt. Brukerens kommentarer etterpå kan tyde på at det var en uklarhet i teksten, og brukeren hadde oppfattet at personen skulle lage fem spørsmål, ikke velge ut fem spørsmål med svar. Det så ikke ut til at andre brukere fant dette forvirrende.

Til tross for at mesteparten av brukerene oppga at de brukte spørsmål de ville huske senere, var det fortsatt enkelte som valgte å legge til hint på et eller flere av spørsmålene. De som la til hint, så på det som en måte for seg selv å komme tilbake til løsningen. En fare med bruk av hint er om de gjør det for enkelt for angripere å finne frem til svaret. Det ble ikke sett på i hvor stor grad hintene her kunne avsløre svaret, men det bør sannsynligvis vurderes slik at brukeren ikke gjør det for enkelt for angripere.

Under innlogging ble hintet for et spørsmål vist direkte under spørsmålet (dog med mindre skriftstørrelse). En av brukerne kommenterte at personen var usikker på hvor hint ble vist, så designet bør presentere hint tydeligere. Det kan også vurderes å ikke vise hint som standard, men ha det tilgjengelig som et valg hvis brukeren har problemer.

Enkelte brukere mente det var en fare for å glemme passord, men så ikke for seg samme trusselen for personlige spørsmål. Også en annen bruker kommenterte at spørsmålene var informasjon som personen ikke ville glemme. En måte å utnytte dette på kunne være å basere spørsmålene på personlige ting som kun brukeren vet, og som personen har visst en lang stund. Et eksempel en av brukerne kom med var at vi ikke vil glemme hva moren vår heter. Selv om kanskje det eksemplet vil være for enkelt for andre å finne ut til at det kan brukes, bør lignende spørsmål vurderes.

Personlige spørsmål var godt likt blant de fleste, men en av brukerene mente det var veldig mye å gjøre. Enkelte av brukerne hadde sett mekanismen før og var kjent med den. Jeg tror spørsmål er en god mekanisme som kan benyttes som et alternativ til passord. Det forutsetter dog et godt utvalg av spørsmål som er vanskelige for andre å gjette, og det er usikkert hvordan det kan beskyttes mot at brukere velger seg lette spørsmål eller svar. Spørsmål vil også innebære at innloggingen tar mer tid enn passord, og særlig registreringen kan ta lang tid. Den store fordelene er brukere kan slippe å lære seg et nytt passord de må huske, og heller basere seg på noe de allerede vet.

6.2.7 Mønstergjenkjenning

Jevnt over var mønster en mekanisme som var godt likt, og spesielt en av brukerne mente mekanismen var uventet og morsom. Men de fleste brukerene tegnet relativt enkle mønstre, og alle holdt seg til minimumsantallet felter, som var kun fem av 25 mulige. Det kan tyde på at grensen som ble satt virket som et akseptabelt minimum, og hva som var nødvendig. En av brukerene kommenterte også under evalueringen at personen ikke så på sikkerheten, siden personen regnet med at eksperter allerede hadde vurdert mekanismene som sikre nok. En annen mulighet er at brukerene tok lettere på sikkerheten

siden de var med i et forsøk og det ikke var en tjeneste de skulle benytte i fremtiden, noe som kan ha påvirket valget deres av mønstre.

Det er likevel oppsiktsvekkende at to brukere tegnet det samme mønsteret med en diagonal strek fra øvre venstre hjørne til nederste høyre hjørne. Også en annen bruker kommenterte at dette var et enkelt mønster som uvedkommende kunne tenke seg å teste først hvis de skulle gjette seg frem til en brukers mønster. Det at dette mønsteret går igjen kan tyde på at det er noe en større mengde brukere vil velge, noe som kan gjøre mekanismen mindre sikker. For passord har det blitt foretatt ulike undersøkelser og samlinger av vanlige og mest brukte passord. Enkelte av disse samlingene har stammet fra angrep der uvedkommende har tatt seg inn og hentet ut all brukerinformasjonen for større nettjenester. I disse samlingene har det vist seg at enkelte enkle kombinasjoner eller ord går igjen. Særlig de samlingene som er hentet fra virkelige tjenester kan gi et innblikk i hvilke passord folk virkelig bruker. Hvis det er sannsynlig brukere vil tegne enkle mønstre på samme måte som en del bruker enkle passord, bør det være mulighet for å legge til rette slik at brukerene oppfordres til å lage sikrere mønstre.

En av brukerene var også bekymret for flere ville tegne symmetriske enn asymmetriske mønstre. Sistnevnte vil være vanskeligere å gjette seg til siden det gir flere muligheter. Også Suo et al [46] tok for seg faren ved symmetriske mønstre. En mulig løsning som ble skildret der var å introdusere et ledd til, ved at brukeren først velger seg ut et område av et større rutenett der brukeren tegner mønsteret sitt. Det blir litt mer for brukeren å huske på, men for uvedkommende øker kompleksiteten skarpt ved at de først må oppdage hvilket område av rutenettet brukeren tegner på og så hvilket mønster brukeren har. Selv om brukeren benytter seg av et enkelt mønster, kan det være vanskelig å vite hvor brukeren tegner det. Igjen kan det oppstå lignende problemer ved at brukere omgår den ekstra sikkerheten ved å velge området øverst i venstre hjørne eller andre, enkle valg.

Sannsynligvis bør det være en mekanisme eller instruksjoner som kan gi brukeren bedre tilbakemelding på hvor sikkert mønsteret er. En mulighet er å legge til instruksjoner for hvilke vanlige mønstre som er usikre, eller en kort animasjon som viser et eksempel på et sikkert mønster. En annen kunne være å gi mulighet å gi brukeren tilbakemelding på hvor sikkert mønsteret er. Tilbakemeldingen bør dekke både hvor enkelt det er å gjette seg frem til det, men bør også inneholde en liste over enkle mønstre som brukerene kan tenkes å benytte seg av. Hvis et kjent mønster benyttes, bør brukeren få tilbakemelding på at det er kjent og det er sannsynlig at andre vil kunne gjette seg til det uten å bruke veldig mye tid eller energi på det.

Samtidig gir mønster store muligheter for kreativiteten til brukerene. Det vil være mulig å tegne symboler, tegn, eller tilsynelatende tilfeldige tegn som

har en mening for brukeren. To av brukerene hadde hver sine systemer for mønster. Den ene baserte seg på et tegn for hver rad, markerte ruter på begge sider og tok utgangspunkt ulik avstand fra kanten for de forskjellige radene. Den andre brukeren baserte seg på hvordan en sjakkbrikke flytter seg. Begge brukerene ga inntrykk av at de hadde valgt systemer de ville huske, mens det var vanskelig for utenforstående å se sammenhengen uten å ha fått en forklaring fra brukerene. Sannsynligvis vil mønstre som har et visst system være vanskeligere å gjette seg frem til for andre enn enklere mønstre.

6.3 Hvilke mentale modeller har brukere for de forskjellige mekanismene og trusselbildet rundt?

I bruk av de ulike autentiseringsmekanismene vil de mentale modellene brukerne danner seg spille inn på deres bruk og oppfattelse av systemet. Det er vanskelig å vite konkret hvordan noen tenker om et spesifikt system, men basert på brukernes uttalelser og observasjoner er det mulig å finne ut mer om hvilke modeller de har.

I brukertesten deltok kun en brukergruppe, nemlig seniorer. Det er vanskelig å si om det er forskjeller blant de forskjellige brukergruppene som fører til at de danner forskjellige mentale modeller av systemet. Dessverre blir det vanskelig å si noe om uten å kunne sammenligne med andre brukergrupper.

6.3.1 Mentale modeller

Brukere danner seg mentale modeller av hvordan systemer fungerer. For at de lettere skal forstå systemet, er det viktig at designerene har lagt opp slik at måten systemet fungerer på overlapper med brukerens modeller av det. Preece et al. [40] hevder at i den virkelige verden danner brukere seg kun et delvis bilde av hvordan systemet fungerer. Det blir dermed utfordrende å ta i bruk all funksjonaliteten i systemet. Videre er det fare for at brukeren kan forme en feilaktig modell, hvis designet er tvetydig, inkonsistent eller obskurt. Siden brukere i stor grad lærer hvordan systemet skal brukes, gjennom nettopp å bruke det, er det viktig at designet kan være med å bygge opp under de riktige modellene. Hvis systemet er i stand til å kommunisere et klart bilde av hvordan det er designet, vil brukeren kunne danne seg en korrekt mental modell, og vil følgende ha en bedre forståelse for systemet.

Opplæring er et aspekt som kan påvirke de mentale modellene, og gi brukerene en bedre presentasjon av hvordan systemet fungerer og hvordan de skulle gå frem. I forbindelse med opplæring i et nytt system, argumenterer Heckle et al [15] for at det er nødvendig å først kjenne til brukerenes eksisterende mentale modeller om autentisering. De eksisterende modellene kan så

brukes i utviklingen av nye systemer, som SSO. Fra overgangen til et system til et annet eller ved introduksjon av nye mekanismer, kan opplæring være et avgjørende punkt. Spesielt hvis avvik mellom brukeres mentale modeller og systemene oppdages, bør de adresseres og opplæringen justeres slik at den bedre kan hjelpe til å forme en korrekt modell.

Preece et al. [40] argumenterer for at å gjøre noe feil i systemet kan være en måte for læring. De viser til at det kan hende brukeren konstruerer en bedre modell over hvordan systemet faktisk fungerer. Ved å gjøre en feil handling som ikke fungerer, kan brukeren oppnå en forståelse for hva personen skulle gjort istedenfor. Dette forutsetter dog at det er enkelt for brukeren å forstå hva som gikk feil, og hvordan problemet kan løses.

For meg virker det sannsynlig at god tilbakemelding i systemet vil kunne være med å hjelpe brukere når han eller hun har gjort noe feil. Hvis brukeren får en forståelse for hva som fungerer i systemet og hva som ikke fungerer, kan bekrefte eller utvide den mentale modellen. Videre kan det trekke opp klarere grenser og en forståelse av hva som er mulig eller ikke mulig i systemet. En fare er at brukerne blir vant til at systemet nekter å utføre de oppgavene de oppfatter som naturlige, slik at de slutter å utforske og gjøre nye ting.

Enkelte av brukerene i brukertesten opplevde mindre problemer eller stod fast, men var i stor grad i stand til å løse problemene selv. Det kan tyde på at de var i stand til å forstå hvordan systemet fungerte, og benytte seg av de tilgjengelige mulighetene for å løse problemene sine. Et eksempel på enkle problemer var brukeren som ved innlogging til bilder først lurte på om mer en et av bildene brukeren hadde valgt ville bli vist. I dette tilfellet så brukeren nærmere på bildene og fant ut like etterpå at kun et av bildene ble vist.

6.3.2 Personlige spørsmål og svar

Under registrering av personlige spørsmål lurte en av brukerne på om knappen merket "legg til" la til bare hintet, eller hva den egentlig gjorde. Brukerens modell var altså uklar i forkant, men knyttet knappen sammen med hint sannsynligvis knappen er plassert like under der hint skrives inn. Etter å ha forsøkt knappen, la brukeren merke til at hele spørsmålet ble lagt til og gjorde så det samme for de øvrige spørsmålene senere. Ved å prøve ut, justerte brukeren sin modell av systemet fra at knappens formål var ukjent til at den la til spørsmål. Med en mer omfattende modell av systemet var det problemfritt å legge til resten av spørsmålene.

En annen bruker så ikke at hint ble vist under spørsmålet ved innlogging, men lurte på om det kanskje ville bli vist hvis brukeren hadde valgt "husker ikke". Denne knappen var derimot ment for å kunne velge et annet spørsmål hvis brukeren ikke husket svaret til det gjeldende. En mulig grunn er at hintet

brukeren har lagt til ikke blir vist tydelig nok, slik at brukeren ikke får god nok tilbakemelding om at det er tatt med til at brukeren legger merke til det. Denne delen kan sannsynligvis forbedres ved å bruke samme skriftstørrelsen på hintet som spørsmålet, eller vurdere å skjule det, helt til brukeren ønsker å vise hintet med en egnet knapp merket "vis hint" e.l. Det er også mulig knappen for å velge et annet spørsmål ikke var tydelig nok, slik at brukerne ikke klarte å plassere hva den gjorde. Det er også mulig at de fleste brukerne ikke tenkte mye over den siden ingen av brukerne så ut til å ha noe bruk for den.

6.3.3 Mønstre

Tegning av mønstre gikk greit, og brukerne så ut til å ha en god forståelse av hvordan de tegnet sitt mønster. En av brukerene uttrykte bekymring for at andre brukere ville velge symmetriske mønstre som var lette å gjette. Også Suo et al [46] antydet at symmetriske mønstre eller figurer ville være svakere enn vanlige passord, mens asymmetriske mønstre ville være sterkere. Et mønster som gikk igjen var en diagonal linje fra øverste venstre hjørne til nedre venstre hjørne. To av brukerne tegnet dette mønsteret, mens en tredje kommenterte det var et enkelt mønster. Det kan tyde på at det er et veldig lett mønster å komme på for flere brukere. På samme måte som enkelte benytter enkle passord som "123" eller rett og slett "passord", er det tenkelig at brukere vil benytte seg av enkle mønstre. Siden det samme mønsteret ble gjentatt flere ganger, kan det være en fare for at brukerne velger seg enkle mønstre, som istedenfor å øke sikkerheten, gjør det enklere for uvedkommende å få tilgang. Sannsynligvis bør mekanismen gi bedre tilbakemelding hvis brukeren velger enkle mønstre om at det vil være lett for andre å gjette seg til.

I forhold til valg av enkle mønstre eller passord, er kanskje en avgjørende del hva brukerne selv oppfatter som enkelt eller vanskelig for andre. Selv brukerne som valgte de enkle mønstre kommenterte i ettertid at de kunne ha valgt mer avanserte mønstre og at det kanskje hadde vært bedre. Det kan tyde på at brukerne har en oppfattelse av at for enkle mønstre vil gjøre det enklere for andre å få tilgang, men det ble ikke avdekket om dette var noe de kom på senere eller om det var noe de var klar over da de valgte spørsmålet. I den virkelige verden er det selvsagt mulig å gå tilbake og endre mønsteret brukt til innlogging, men det er ukjent om brukere ville benyttet seg av denne muligheten hvis de oppdager at mønsteret de bruker er enkelt å gjette eller om de beholder det fordi de anser risikoen som liten.

6.3.4 Klare instruksjoner

Underveis i testene ble det oppdaget at enkelte av instruksjonene var uklare og kunne virke villede på brukerne. Teksten for å fjerne bilder fra et utvalg i bilder eller lyder, og knappen for å nullstille mønster var i utgangspunktet skrevet som en ordre. I pilottesten fjernet derfor personen bildene sine igjen etter å ha valgt de. Personen var forvirret over hvorfor det skulle gjøres, men hadde fulgt instruksjonene på skjermen. I forhold til brukerens modell hadde brukeren fått instruksjoner om å først velge fem bilder, og lengre nede på siden stod det brukeren skulle klikke på bildene i utvalget for å fjerne dem igjen. I utgangspunktet er det ingen forskjell på de to instruksjonene siden det ikke kommer frem at den nederste instruksjonen er valgfritt å gjennomføre. Dette fører til en mismatch mellom hvordan systemet fungerer og hva brukeren oppfatter. Men det kan argumenteres med at brukerens oppfatning er korrekt siden instruksjonene er skrevet på den måten de er. Denne teksten ble justert for at brukerne skulle få et mer korrekt inntrykk av at det var en mulighet hvis brukeren angret på et eller flere av bildene som ble valgt. Etter at tekstene ble endret, var det ingen av brukerne som benyttet seg av den. Sannsynligvis så de ikke noen grunn til å bytte det de hadde valgt, men det var heller ingen som fikk feil oppfatning og fjernet alle bildene sine igjen.

Et annet sted som var litt uklart var under innlogging med lyder. En av brukerne pekte ut at overskriften kun sa at brukerne skulle velge en lyd, uten at det ble spesifisert at det var brukerens lyd det var snakk om. Personen forstod hva som var intensjonen, men gikk likevel igjennom og valgte tilfeldige lyder for å demonstrere hva brukere som kun fulgte instruksjonene kunne gjøre. I dette tilfellet var brukerens modell korrekt på tross av den feilaktige instruksjonen, og det var heller ingen andre brukere som ikke forstod de skulle velge sine bilder. Likevel er det viktig å få rettet opp slik at instruksjonene er korrekte for at de kan støtte opp om den korrekte modellen.

6.3.5 Lyder og kategoriene

Den delen som klart flest brukere hadde problemer med var de forskjellige kategoriene av lyder. Kun en av brukerne skiftet kategori. Det må dog merkes at dette var pilottesten, som også hadde flere kategorier å velge mellom for bilder, der brukeren forsøkte å velge et bilde fra hver kategori. Brukeren forsøkte å bruke den samme fremgangsmåten her, og det er mulig dette valget eller at brukeren hadde byttet mellom kategorier i bilder var utslagsgivende. De andre brukerne så ikke på lydene i de andre kategoriene engang selv om en kommenterte at det var flere kategorier etter å ha lest instruksjonene og en annen lurte på hva bildene på venstresiden gjorde etterpå.

Som foreslått tidligere er det mulig bedre tilbakemelding om de mulige kategoriene og at lydene fra en spesifikk kategori blir vist nå kunne hjulpet. Enten ved å legge til tekst i tillegg til bilde på de forskjellige kategoriene for å gi mer informasjon, eller legge til tekst over kategoriene som oppfordrer til å bytte kategori eller forteller hvilken kategori som er gjeldende. Disse kunne gjort det klarere hva bildene på siden var, slik at brukerne kunne dannet seg et bedre bilde av at de var mulige å trykke på og hva som ville skjedd.

En annen mulighet ville så klart vært å vise alle lydene samlet siden brukerne ikke så ut til å ha noen problemer med det for bildene. Men noe av poenget med å beholde kategoriene var å kunne sammenligne hvilket av de to oppsettene brukerne foretrekte. Basert på undersøkelsen her tyder på at de foretrakk å ha utvalget samlet. På den annen side kan også være at implementasjonen av kategorier var dårligere, og at designet bør styrkes gjennom noen av forslagene ovenfor.

Lyd var den dårligst likte mekanismen. Det er usikkert hvor mye av dette inntrykket som kommer fra dyrelydene som ble vist som standard. Det er usikkert om bruk av andre lyder ville gitt det samme resultatet. Men enkelte brukere kommenterte også at de ikke helt så poenget med å bruke lyd til innlogging, så det er mulig mekanismen simpelthen ikke egnet seg for dem.

6.3.6 Snarveier

I tilfeller hvor sikkerhetsmekanismene blir for avanserte eller tungvinte, kan det tenkes brukere forsøker å ta snarveier for å få gjort det de skal. Enkelte går så langt som å hevde at sikkerhetssystemer kan sees på som en kneik brukeren må over for å komme i gang med det personen skal [15]. Brukere ser ut til å vurdere oppgavene de skal ha gjort over sikkerheten, og det mest kjente eksemplet er kanskje passord som blir skrevet ned istedenfor at brukeren skal huske dem. Særlig i tilfeller hvor brukerne bruker passordet sjeldent eller har flere passord å holde orden på. Dessverre fører dette i praksis til at sikkerheten synker, på tross av de sikre passordene i tråd med gjeldende policy. Et kjent eksempel er om kravene for passord blir for kompliserte ender passordene opp på en lapp ved siden av skjermen, siden brukeren ikke klarer å huske passordet. For at brukeren skal kunne utføre sine vanlige arbeidsoppgaver blir sikkerheten redusert, stikk i strid med intensjonene rundt passordkrav.

I forbindelse med brukertesten så det ut som om enkelte av brukerne valgte utifra hva som minimum var nødvendig. Spesielt for mønster der det var angitt å merke minst fem ruter, var det ingen brukere som merket fler. Det var også en bruker som telte opp hvor mange tegn passordet sitt inneholdt, sannsynligvis for å forsikre seg om at det var nok. Slike valg kan tyde på at brukerne ser liten verdi i å investere i sikkerheten utifra hva som er

minimum tjenesten tillater. Men et interessant aspekt er at flere gikk utifra at løsningene var sikre når de skulle vurderes, og en person regnet med at sikkerhetseksperter allerede hadde vurdert om mekanismene var sikre eller ikke før det blir tatt i bruk. Hvis brukerne har oppfatningen at minimumskravet er en grense satt av noen som har avgjort at det er en grense for at passordet e.l. skal være sikkert er det mulig de går utifra at det er alt som kreves. Når brukerne allerede har et forslag som oppfyller minimumskravet, ser det ut som om de ikke ser nytten i å gjøre det mer komplisert.

Dette kan indirekte skyldes at de har andre passord fra før av de skal huske på i tillegg, men det kan også komme an på hvordan de ser grensen for minimumskravet. Det er to måter å se sikkerhetskravet for f.eks. tegn i passord, den ene er at fra dette punktet er løsningen sikker og den andre er at opp til dette punktet er løsningen usikker. De som ser det på den første måten kan tenke seg vil legge til flere tegn for å øke sikkerheten, mens de av den andre oppfatningen har sørget for at passordet ikke er usikkert, ergo må det være sikkert. Med lite tilbakemelding utover om minimumskravet er oppfylt eller ikke kan dette bli en avgjørende faktor for om brukeren avgjør passordet er sikkert nok. I brukertesten ble brukerne ikke spurt hvordan de vurderte kravene, om de virket fornuftige, strengere eller svakere enn nødvendig. Det er derfor vanskelig å si noe nøyaktig om brukernes syn på minimumskrav.

6.3.7 Syn på trusler

Et element av sikkerheten er de mulige truslene. For at sikkerheten skal fungere er det viktig at brukerne kjenner til de truslene som finnes og tar sine forhåndsregler for å unngå dem. Autentiseringsmekanismene er et ledd i å skille mellom legetime brukere og uvedkommende, men for å best mulig kunne gjøre dette krever det at brukerne velger gode passord eller tilsvarende slik at det blir vanskeligere for uvedkommende å få tilgang.

I en undersøkelse om sikkerhet for trådløse nettverk, fant Klasnja et al [19] at brukerne så på uvedkommende som bryter seg inn i maskinene deres som den største trusselen. Det ble likevel sett på som lite sannsynlig, siden de så for seg at det krever en angriper med gode kunnskaper. En annen trussel som kom frem i undersøkelsen var andre som kunne se hva de gjorde på maskinen hvis de befant seg på et offentlig sted.

Under vurderingen av de forskjellige mekanismene, ble brukerne spurt hvordan de så for seg at uvedkommende kunne logge seg inn med de forskjellige mekanismene. De fleste så for seg at en angriper ville forsøke å gjette seg frem til passordet de hadde, eller kombinasjonen av bilder/lyd osv de hadde registrert. En del av dem hadde også oppfatningen av enkelte mekanismer, ofte personlige spørsmål, ville være umulige for andre å gjette seg frem til.

Det at de la vekt på gjetting kan være et tegn på hull i trusselbildet. Mange av angrepene mot passord baserer seg snarere på ordbøker eller ferdige lister med ofte brukte passord, som kanskje er vanskeligere å se for seg.

Likevel kommenterte enkelte av brukerne at hvem angriperen var ville ha noe å si. En bruker kommenterte at hvis det var noen som kjente personen godt, ville de muligens kjenne svaret på de personlige spørsmålene. En annen mente at det ville være teoretisk mulig for andre å finne passordet eller svar på personlige spørsmål. Personen hadde likevel tiltro til passordsystemet sitt, og mente det ville være godt gjort av uvedkommende hvis de fant ut hvordan personen tenkte. Jeg anser dette som en grei vurdering siden det virker som brukerne er klare over at en angriper kan være noen som kjenner dem eller kan ha tilegnet seg kunnskap om brukeren. Særlig med tanke på personlige spørsmål er angripere som kjenner brukeren godt sannsynligvis bedre i stand til å vite svaret på spørsmålene enn en tilfeldig angriper vil være. Men kombinert med at brukerne ikke nevnte automatiserte angrep er det mulig de overvurderer sikkerheten til passordene sine. Det er dog vanskelig å kontrollere uten å sjekke selve passordene om de ville være enkle å finne ut av med automatiske angrep eller ikke.

Ingen av brukerne virket betenkte med at flere av mekanismene vises i klartekst, i motsetning til Klasnja et al [19] der brukerne nevnte at andre kunne se hva de gjorde på maskinen som en mulig trussel. Siden det tydelig vises på skjermen vil det være mulig for andre i bakgrunnen å se hva brukerne gjør. Det er usikkert om brukerene har unnlatt å nevne ulike trusler fordi de ikke er klar over de potensielle truslene eller fordi de oppfatter at de er beskyttet mot dem. Bortsett fra enkelte som kommenterte kjennskap til brukeren, var det ingen som nevnte at angripere kunne se over skulderen når brukeren skrev inn eller klikket på elementer på skjermen for å logge seg inn. Det er mulig at brukerene i stor grad bruker maskinene sine hjemme eller omgivelser der de har oversikt over hvem andre som er til stede og stoler på disse personene, men det kan også være en del av trusselbildet brukere ikke har sett for seg. Etter at testlederen nevnte muligheten for innlogging med lyder, og hva de tenkte om andre personer i rommet når lydene ble spilt av, innså de fleste at de rundt kunne høre lydene. Men det var ingen som fulgte opp med lignende elementer for de andre mekanismene.

Det var en rekke andre mulige trusler som heller ikke ble nevnt. F.eks. ble ikke mer målrettede angrep som virus, spionvare eller phishing nevnt, enda særlig sistnevnte svært utbredte [5]. Igjen er det usikkert om det var fordi brukerene ikke var klar over dem, ikke husket dem er og da, eller anså seg som beskyttet mot slike trusler. En av brukerne som brukte egen maskin hadde nettopp installert oppdateringer til antivirus-programmet sitt, og nevnte viktigheten av å holde dem oppdatert. Det kan tyde på at brukerne

er klar over flere trusler enn de som ble nevnt under evalueringen.

En kommentar som gikk igjen for flere brukere var at f.eks. avanserte mønstre vil være vanskeligere for andre å gjette seg til, men samtidig vanskelig å huske. For at brukerne i det hele tatt skal kunne huske mønsteret (eller passordet) sitt kan det ikke være for komplisert. Allikevel bør det være vanskelig nok til at uvedkommende ikke kan finne det ut. Måten brukerne så på denne avveiningen vitner om at de ser problemstillingen, men prioriterer seg selv, slik at de selv er i stand til å bruke systemet. Det var også skiller på hvilke mekanismer som ble sett på som sikrere enn andre. Noen av brukerne mente personlige spørsmål var umulige for andre å gjette seg til, mens en bruker mente det ville vært enkelt. Til en viss grad vil det selvfølgelig avhenge av spørsmålene brukerne velger og hvor lett det er å finne informasjon om f.eks. navn på brukerens slektninger eller tidlige kjæledyr. Som noen av brukerne nevnte, kommer det veldig an på hvem angriperen er og om personen kjenner brukeren fra før. Det kan tenkes at en nær venn eller familiemedlem vil i større grad finne eller vite svarene til brukerens personlige spørsmål enn utenforstående.

Som Suo et al [46] nevnte er enkelte mekanismer mer motstandsdyktige mot former for sosial manipulering ved at det er vanskeligere å oppgi et grafisk passord over telefonen, men vil fortsatt gjøre lite for å hindre phishing.

7 Konklusjon

Hvilke ulike autentiseringsmekanismer er i bruk eller kan benyttes per i dag?

Vi har sett på og diskutert forskjellige autentiseringsmekanismer fra litteraturen og prototypen. Det har blitt foreslått en rekke forskjellige mekanismer, som grafiske passord, innlogging med lyd eller ved registrering av biometriske trekk. Flere av disse mekanismene virker lovende og kan være tilgjengelig som alternativer eller i tillegg til passord. Grunnen til å se på disse mekanismene er for å gjøre det lettere for brukere som har problemer med et stort antall passord til forskjellige nettsteder og tjenester. Det kan også tenkes ulike tjenester med forskjellige sikkerhetsnivåer kan tilby alternativer for brukere som ønsker det. Til slutt kan enkelte former, som innlogging med lyd, gjøre hverdagen enklere for blinde og svaksynte ved at de får en bedre tilpasset mekanisme de kan ta i bruk.

Blant de grafiske passordene, er tegning av mønster en mulighet. Noen implementasjoner ble ansett som like sikre som vanlig passord, men var dessverre veldig avhengig av hvilke mønstre brukerne tegnet.

Hvordan fungerer et utvalg av av disse mekanismene under utprøving med brukere i praksis?

Fra brukertesten ble følgende mekanismer prøvd ut av fem seniorbrukere; passord, bildegjenkjenning, lyd, personlige spørsmål og mønster. Det viser seg at kategoriene i lyder var problematiske, siden få av brukerne forstod hvordan kategoriene ble brukt. Samtidig så vi at mange av brukerne likte mekanismer som bilder og personlige spørsmål, selv om enkelte hadde litt problemer med bruken av førstnevnte. Alt i alt virket brukerne åpne for å ta i bruk de alternative mekanismene, som enkelte mente var bedre enn passord. De fleste fikk til innlogging på første forsøk, men enkelte av mekanismene var litt vanskeligere eller tok lengre tid i registreringen.

Passord var likevel en av de best likte mekanismene, sammen med personlige spørsmål. Mens meningene var delte om mønster, var de minst foretrukne mekanismene bilder og lyd. Få av brukerne hadde problemer med passord, på tross av kravene om lengde og kombinasjon av tall. Mange likte tegning av mønster og en bruker synes den var morsom. Dessverre brukte mange av brukerne enkle mønstre som er lette å gjette seg til, så det bør sees nærmere på hvordan det kan forhindres. Likedan valgte mange det norske flagget i bildeutvalget, som kan tyde på at enkelte bilder vil velges av mange brukere som gjør det enklere å gjette at det er brukt.

Hvilke mentale modeller har brukere for de forskjellige mekanismene og trusselbildet rundt?

Brukernes mentale modeller så ut til å for det meste overlappe godt med systemet. Enkelte hadde mindre problemer der de selv fant løsninger og justerte modellene sine til å være mer korrekte, men det var også et par ting brukerene stilte spørsmål om. I stor grad gjorde brukerne dette på egen hånd med den informasjonen som var tilgjengelig i systemet og de tilbakemeldingene de fikk.

Et av de tydeligste problemene var kategoriene ved valg av lyd. Kun en av testpersonene fant ut hvordan det var mulig å bytte til andre kategorier. De andre valgte kun lyder fra standardkategorien som ble først vist. Det kan tyde på at implementasjonen ikke presenterte klart nok hvordan det var mulig å bytte til andre kategorier eller at det ikke kommuniserte godt nok til brukerne at flere kategorier i det hele tatt var tilgjengelige.

Enkelte områder av prototypen inneholdt vage instruksjoner, som gjorde det mulig for brukere å danne seg en feilaktig modell. Teksten for å endre bilder eller lyder som ble valgt kunne tolkes som en ordre eller steg som skulle gjennomføres, noe som gjorde at en bruker fjernet alle bildene personen hadde valgt. Ved å rette opp teksten til å bedre signalisere det var en mulighet unngikk andre brukere det samme problemet. Ved å bedre informere om hvilke muligheter som var i systemet og justere brukerens modell i forhold til systemet hadde de andre brukerne et bedre utgangspunkt.

Brukerenes syn ser for seg trusler i form av at andre skal gjette informasjonen de bruker for å logge seg inn. De har ulik tro på hvilke mekanismer som er sikrest, men de fleste mener hvem angriperen er har mye å si. Noen som kjenner brukeren bedre vil ha bedre forutsetninger til å vite hva brukeren foretrekker, eller svar på personlige spørsmål osv. Det var en rekke trusler brukerne ikke nevnte, men det er usikkert om de ikke vet om dem eller at de simpelthen ikke ble nevnt i denne sammenhengen.

7.1 Videre forskning

Selv om mye har blitt kartlagt i denne oppgaven, er det fortsatt områder som kan være aktuelle å se nærmere på i fremtidene. Først og fremst finnes det flere mekanismer som kan sees på. Det er sannsynligvis flere alternative mekanismer som ikke har blitt dekket her. Basert på historiske kunnskap og bla. denne oppgaven, har vi forhåpentligvis en bedre ide om hvilke område man kan se til og hvilke løsninger som kan vurderes.

Dessverre fikk jeg ikke tid til å være med på brukertester med andre brukergrupper som dyslektikere og blinde og svaksynte. Jeg tror tester med

flere brukergruppere ville gjort det mulig å avdekke om prototypen inneholder flere problemområder. Det ville også vært interessant å sett hvor like eller ulike resultatene ville blitt med andre brukergrupper. Dette er tester som er planlagt i forskningsprosjektet, men som jeg ikke rakk å være med på før oppgaven skulle leveres.

På grunn av en del begrensninger, mekanismene kun blitt forsøkt alene. Det ville vært interessant å prøvd dem ut i større skala, kanskje knyttet til en tjeneste der brukeren har mulighet til å velge blant autentiseringsmekanismene. Dette krever selvfølgelig en løsning eller tjeneste som er villig til å satse på å benytte alternative autentiseringsmekanismer. Hvis dette ble gjennomført burde resultatene bli dokumentert for å se hvordan det fungerer for større løsninger også i den virkelige verden.

Underveis i prosjektet hadde jeg veldig lyst til å se nærmere på SSO, både hvordan det fungerer og hvordan brukere oppfatter det når de kan logge inn flere steder med samme informasjon. Hvordan brukerne ser for seg at informasjonen lagres eller de ulike tjenestene er knyttet sammen kan være interessant for videre utvikling av SSO og de metaforer som bør benyttes for å gi brukerne en klarere forståelse. SSO var i utgangspunktet planlagt, men ble utsatt i forskningsprosjektet jeg var med i, så siden jeg ville få lite konkret materiale å diskutere, droppet jeg denne delen.

Trusselbildet brukerne har bør sannsynligvis studeres i nærmere detalj. Denne oppgavene kan tyde på noen områder som brukerne er klar over, mens andre ikke ble nevnt. Siden det er usikkert om dette er fordi brukerne ikke er klar over disse truslene eller simpelthen fordi de ikke nevnte dem bør sees nærmere på Samtidig kan det være interessant å se på hvordan krav for de ulike mekanismene og tilbakemeldingene brukerne får gjør dem bedre rustet i forhold til de forskjellige truslene. Hvordan kan tilbakemeldingene bedre gjenspeile hvor godt brukerne er beskyttet og hvordan kan eventuelt brukerne gjøres oppmerksomme på mulige trusler og risikoer gjennom autentiseringsmekanismene?

Referanser

[1] Anne Adams and Martina Angela Sasse. Users are not the enemy. *Commun. ACM*, 42:40–46, December 1999.

[2] Ronald M. Baecker, Jonathan Grudin, William A. S. Buxton, and Saul Greenberg. *Human-computer interaction Toward the year 2000*. Morgan Kaufmann Publishers,Inc, 1995.

[3] Vannevar Bush. As we may think. *interactions*, 3:35–46, March 1996.

[4] L.J. Camp. Mental models of privacy and security. *Technology and Society Magazine, IEEE*, 28(3):37 –46, 2009.

[5] Torgeir Daler, Roar Gulbrandsen, Tore Audun Høie, and Torbjørn Sjølstad. *Håndbok i datasikkerhet – informasjonsteknologi og risikostyring 2.utgave*. Tapir Akademisk Forlag, 2006.

[6] Laura DeNardis. A history of internet security. In Karl de Leeuw and Jan Bergstra, editors, *The History of Information Security A Comprehensive Handbook*, pages 681–704. Elsevier, 2007.

[7] Alan Dix, Janet Finlay, Gregory Abowd, and Russell Beale. *Human-Computer Interaction*. Prentice Hall, 1993.

[8] Hossein Bidgoli (ed.). *Encyclopedia of Information Systems*. Academic Press, 2003.

[9] Alain Forget and Robert Biddle. Memorability of persuasive passwords. In *CHI '08 extended abstracts on Human factors in computing systems*, CHI '08, pages 3759–3764, New York, NY, USA, 2008. ACM.

[10] Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu, and U. Aickelin. A new graphical password scheme resistant to shoulder-surfing. In *Cyberworlds (CW), 2010 International Conference on*, pages 194 –199, 2010.

[11] Shirley Gaw and Edward W. Felten. Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security*, SOUPS '06, pages 44–55, New York, NY, USA, 2006. ACM.

[12] T. Gilb. Point/counterpoint. *Software, IEEE*, 25(2):64 –67, 2008.

[13] Stefano Grazioli and Sirkka L. Jarvenpaa. Deceived: under target online. *Commun. ACM*, 46:196–205, December 2003.

[14] Gisle Hannemyr. Personvern i deltakerskapte, rike medier. In Heidi Grande Røys, editor, *Delte meninger*. Universitetsforlaget, 2009.

[15] Rosa Heckle, Wayne G. Lutters, and David Gurzick. Network authentication using single sign-on: the challenge of aligning mental models. In *Proceedings of the 2nd ACM Symposium on Computer Human Interaction for Management of Information Technology*, CHiMiT '08, pages 6:1–6:10, New York, NY, USA, 2008. ACM.

[16] Thomas Hoff. En økologisk tilnærming til visuell persepsjon. `http://www.svt.ntnu.no/psy/Thomas.Hoff/Artikler/GIBSON.html`.

[17] A.K. Jain, A. Ross, and S. Pankanti. Biometrics: a tool for information security. *Information Forensics and Security, IEEE Transactions on*, 1(2):125 – 143, 2006.

[18] Mark Keith, Benjamin Shao, and Paul John Steinbart. The usability of passphrases for authentication: An empirical field study. *Int. J. Hum.-Comput. Stud.*, 65:17–28, January 2007.

[19] Predrag Klasnja, Sunny Consolvo, Jaeyeon Jung, Benjamin M. Greenstein, Louis LeGrand, Pauline Powledge, and David Wetherall. "when i am on wi-fi, i am fearless": privacy concerns & practices in eeryday wi-fi use. In *Proceedings of the 27th international conference on Human factors in computing systems*, CHI '09, pages 1993–2002, New York, NY, USA, 2009. ACM.

[20] Det kongelige fornyings-og administrasjonsdepartement. *Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor Retningslinjer for offentlige virksomheter som tilrettelegger elektroniske tjenester og samhandling på nett*. 2008.

[21] D. Kristol and L. Montulli. Http state management mechanism, 1997.

[22] D. Kristol and L. Montulli. Http state management mechanism, 2000.

[23] Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Lawrence G. Roberts, and Stephen S. Wolff. The past and future history of the internet. *Commun. ACM*, 40:102–108, February 1997.

[24] C. Maple and P. Norrington. The usability and practicality of biometric authentication in the workplace. In *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*, page 7 pp., 2006.

[25] Job Mashapa and Darelle van Greunen. User experience evaluation metrics for usable accounting tools. In *Proceedings of the 2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists*, SAICSIT '10, pages 170–181, New York, NY, USA, 2010. ACM.

[26] David E. Millard and Martin Ross. Web 2.0: hypertext by any other name? In *Proceedings of the seventeenth conference on Hypertext and hypermedia*, HYPERTEXT '06, pages 27–30, New York, NY, USA, 2006. ACM.

[27] S. Muhammad, Z. Furqan, and R.K. Guha. Designing authentication protocols: Trends and issues. In *Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, 2006. ICN/ICONS/MCL 2006. International Conference on*, page 76, 2006.

[28] Brad A. Myers. A brief history of human computer interaction technology. 5(2):44–54, March 1998.

[29] B.C. Neuman and T. Ts'o. Kerberos: an authentication service for computer networks. *Communications Magazine, IEEE*, 32(9):33 –38, September 1994.

[30] Jacob Nielsen. How to conduct a heuristic evaluation.

[31] Donald A. Norman. Affordance, conventions, and design. *interactions*, 6:38–43, May 1999.

[32] Donald A. Norman. Human-centered design considered harmful. *interactions*, 12:14–19, July 2005.

[33] Donald A. Norman. The way i see it: When security gets in the way. *interactions*, 16:60–63, November 2009.

[34] Donald A. Norman. Natural user interfaces are not natural. *interactions*, 17:6–10, May 2010.

[35] Donald A. Norman. The way i see it: Looking back, looking forward. *interactions*, 17:61–63, November 2010.

[36] Tim O'Reilly. What is web 2.0: Design patterns and business models for the next generation of software. Mpra paper, University Library of Munich, Germany, 2007.

[37] Shari Lawrence Pfleeger. Design and analysis in software engineering: the language of case studies and formal experiments. *SIGSOFT Softw. Eng. Notes*, 19:16–20, October 1994.

[38] Vir V. Phoha. *Internet Security Dictionary*. Springer, 2002.

[39] Stefanie Pötzsch, Peter Wolkerstorfer, and Cornelia Graf. Privacy-awareness information for web forums: results from an empirical study. In *Proceedings of the 6th Nordic Conference on Human-Computer Interaction: Extending Boundaries*, NordiCHI '10, pages 363–372, New York, NY, USA, 2010. ACM.

[40] Jenny Preece, Yvonne Rogers, Helen Sharp, David Benyon, Simon Holland, and Tom Carey. *Human-computer interaction*. Addison Weasly Longman Limited, 1994.

[41] Bart Preneel. An introduction to modern cryptology. In Karl de Leeuw and Jan Bergstra, editors, *The History of Information Security A Comprehensive Handbook*, pages 565–592. Elsevier, 2007.

[42] K.R. Radhika, G.N. Sekhar, and M.K. Venkatesha. Server-side reconstruction trajectory generation methods for hand written objects authentication - a comparative review. In *Multimedia Computing and Systems, 2009. ICMCS '09. International Conference on*, pages 211 –215, 2009.

[43] S.N.S.M. Saei, S. Sulaiman, and H. Hasbullah. Mental model of blind users to assist designers in system development. In *Information Technology (ITSim), 2010 International Symposium in*, volume 1, pages 1 –5, 2010.

[44] A. Sharma, V. Ojha, R.C. Belwal, and G. Agarwal. Password based authentication: Philosophical survey. In *Intelligent Computing and Intelligent Systems (ICIS), 2010 IEEE International Conference on*, volume 3, pages 619 –622, 2010.

[45] Ben Shneiderman. Understanding human reactivites and relationships: an excerpt from leonardo's laptop. *interactions*, 9:40–53, September 2002.

[46] Xiaoyuan Suo, Ying Zhu, and G.S. Owen. Graphical passwords: a survey. In *Computer Security Applications Conference, 21st Annual*, pages 10 pp. –472, 2005.

[47] J. Torres, J.M. Sierra, and A. Izquierdo. A realistic approach on password-based mutual remote authentication schemes with smart-cards. In *Digital EcoSystems and Technologies Conference, 2007. DEST '07. Inaugural IEEE-IES*, pages 334 –338, 2007.

[48] Janice Y. Tsai, Patrick Kelley, Paul Drielsma, Lorrie Faith Cranor, Jason Hong, and Norman Sadeh. Who's viewed you?: the impact of feedback in a mobile location-sharing application. In *Proceedings of the 27th international conference on Human factors in computing systems*, CHI '09, pages 2003–2012, New York, NY, USA, 2009. ACM.

[49] Alma Whitten and J. D. Tygar. Why johnny can't encrypt. In *In Proceedings of the 8th USENIX Security Symposium*, 1999.

[50] J.M. Wing. A symbiotic relationship between formal methods and security. In *Computer Security, Dependability and Assurance: From Needs to Solutions, 1998. Proceedings*, 1998.

[51] Jeffrey R. Yost. A history of computer security standards. In Karl de Leeuw and Jan Bergstra, editors, *The History of Information Security A Comprehensive Handbook*, pages 595–621. Elsevier, 2007.

[52] Gang Zhao, Dong Zheng, and Kefei Chen. Design of single sign-on. In *E-Commerce Technology for Dynamic E-Business, 2004. IEEE International Conference on*, pages 253 –256, 2004.

Appendiks A: Spørsmål til autentiseringsmekanismene

Brukerene ble stilt disse spørsmålene for hver mekanisme etter å ha gått igjennom dem. I enkelte tilfeller ble noen av svarene fulgt opp med tilleggspørsmål, som ikke var avtalt på forhånd.

1. Hvordan likte du denne metoden for innlogging? Meget godt (=1) Godt (=2) Ikke så godt (=3) Veldig dårlig (=4)
2. Hvorfor likte du innloggingen... (svar på spørsmålet over)?
3. Hvor lett var det å skjønne hva du skulle gjøre? Meget lett (=1) Lett (=2) Litt vanskelig (=3) Meget vanskelig (=4)
4. Lurte du på noe underveis? I så fall hva?
5. Hvordan fant du svaret på det du lurte på?
6. Hvordan tenkte du da du valgte hva du skulle huske?

Appendiks B: Spørsmål til evaluering av mekanismene

Spørsmål brukeren ble stilt etter å ha vurderte mekanismene. Også her kunne enkelte svar bli fulgt opp med ekstraspørsmål.

1. Hvorfor likte du metode X best?
2. Hvorfor likte du metode Y dårligst?
3. Hva har vært viktigst for deg når det gjelder rangering av metodene?(Stikkord: Enkelt, sikkert, lite å skrive, lite å lese, rask, lett å forstå, tror du husker det du skal)
4. For hvilken metode tror du uvedkommende lettest kan finne ut hva du har valgt? På hvilken måte?
5. Var det noe som var vanskelig å forstå i testen (ble kun stilt til pilottesteren)?
6. Hva syns du kan gjøres bedre med denne testen (ble kun stilt til pilottesteren)?