NTNU
Det skapende universitet

Brukervennlig og sikker innlogging på sykehus: dagens praksis og forslag til alternative løsninger

Endre Fuglseth

Master i informatikk
Oppgaven levert: Juni 2008
Hovedveileder: Dag Svanæs, IDI

Norges teknisk-naturvitenskapelige universitet
Institutt for datateknikk og informasjonsvitenskap

NTNU
Fakultet for informasjonsteknologi,
matematikk og elektroteknikk
Institutt for datateknikk
og informasjonsvitenskap

MASTEROPPGAVE

Brukervennlig og sikker innlogging på sykehus: dagens praksis og forslag til alternative løsninger

Endre Fuglseth

Veileder: Dag Svanæs

Dato: 15. juni 2008

Norges Teknisk- Naturvitenskaplige Universitet
Institutt for datateknikk og informasjonsvitenskap

Forord

Denne oppgaven startet med en samtale med min veileder Dag Svanæs der han introduserte meg for problematikken med innlogging på St.Olavs hospital. Jeg har gjennom hele mitt informatikkstudie vært opptatt av viktigheten av gode brukergrensesnitt og at bruker og oppgaven brukeren skal utføre settes i fokus. Derfor virket denne problemstillingen som en veldig interessant utfordring siden jeg da ville kunne jobbe innenfor brukersentrert design og samtidig kunne få se teknologi i bruk i et hektisk sykehusmiljø.

Endre Fuglseth
Trondheim, mai 2008

Takk til

Takk til sykepleiere, hjelpepleiere og leger på Nevrologisk sengepost ved St.Olavs hospital for tålmodighet og hjelpsomhet under observasjoner og intervjuer. Setter også stor pris på all hjelp og oppmuntring jeg har fått hos min veileder Dag Svanæs og de tilknyttet Norsk Senter for Elektronisk Pasientjournal (NSEP), inkludert Arild Faxvaag. Til slutt vil jeg takke mine venner og min forlovede for forståelse og støtte gjennom oppgaveprosessen.

Innhold

Sammendrag

Teknologiske fremskritt innenfor autentiseringsteknologi gir nå nye muligheter i utallige bruksområder. Grunnet rapportering av ugunstige løsninger [12] er det også nå ønskelig å kunne ta i bruk nye teknologiske løsninger på sykehus der behovet for rask tilgang til ressurser og dokumentasjon av journal-endringer er særdeles viktig samtidig som man må opprettholde sikkerheten [4].

I dette studiet vil vi utføre en observasjon og av datasystemet i bruk og innloggingsrutiner ved Nevrologisk Avdeling, St.Olavs Hospital, Trondheim for å kunne avdekke problemområder og komme med forslag til nye løsninger ved bruk av ny teknologi.

Observasjonene avdekket at dagens løsning krever at de har kortet i maskinen for å være innlogget. Tidligere studier som [4] har også pekt på lignende problemer ved tidligere studier. Dette studiet fant lignende problemer ved det sykehuset som observasjonene ble gjort på, men i tillegg var det en del nye problemområder som dukket opp. Ved å ta i bruk ny teknologi for innlogging vil hverdagen til sykehusansatte forhåpentlig forbedre seg, spesielt med tanke på at det har blitt gjort vellykkede forsøk med bruk av slik teknologi tidligere.

Ved bruk av resultatene fra observasjoner og intervju ble det avdekket en rekke problemer relatert til innlogging. Krav til løsning ble utarbeidet og forslag til nye løsninger ble sammenlagt på bakgrunn av kravene og sammenligninger av teknologi som ble gjort i første del av oppgava

Resultatene av dette studiet er ment som en veiledning for design og utvikling av innloggingssystemet ved St.Olavs Hospital og andre sykehus i tillegg til andre institusjoner som har nytte av slik teknologi.

Nøkkelord: Innlogging, autentisering, brukervennlighet, sikkerhet, observasjon, intervju, helsesektor, sykehus

Kapittel 1

Innledning

Å gjenkjenne mennesker har alle tider vært essensielt innen sikkerhet. Et adgangskontrollsystem skal kunne kjenne igjen personale for å sikre verdier eller personopplysninger. Det er dette skal sees nærmere på i denne masteroppgaven, med fokus i anvendelse på sykehus og hvilken teknologi som best dekker behovet i en hektisk hverdag for sykehusansatte.

På et sykehus er det viktig å kunne korrekt identifisere ansatte for å finne ut hvilke steder og ressurser de har adgang til. Det er til avdelinger, undersøkelsesrom, kontorer, lager, medisinrom, eller andre rom som inneholder personal- eller pasientopplysninger eller kostbart utstyr som må beskyttes. Nå med overgangen til elektroniske pasientjournaler kreves det ytterligere sikkerhetsrutiner for å kontrollere adgang til datasystemet enn før. Med sensitiv informasjon koblet opp mot Internett og terminaler rundt om i sykehuset har adgangskontroll blitt høy prioritet. Spesielt med tanke på at adgang til terminalene på sykehuset kan lett bli gjort tilgjengelig for uvedkommende, spesielt hvis de er innlogget og brukeren har forlatt stasjonen åpen.

På alle sykehus er det nå en selvfølge med system i høyeste klasse for adgangskontroll både på dører og på datasystemet. Det jobbes hele tiden med forbedringer og nye løsninger, og det er mange prosjekter i gang både i innland og utland. Men uansett hvor høyteknologiske løsninger man bruker i et sikkerhetssystem vil ikke systemet være helt sikkert hvis man ikke inkluderer personalet som en del av sikkerhetssystemet. Dette er nok de fleste klar over, og sykehuspersonale har stor respekt for taushetsplikten sin. Men viss sikkerhetsløsningene gjør hverdagen til sykehusansatte veldig tungvinte, vil de ansatte etter hvert gå rundt sikkerhetsrutinene. Dette gjør de ikke fordi de ikke har respekt for sikkerheten eller at de er slurvete, men de gjør det for at det ikke skal gå utover pasientene og for at de i det hele tatt skal få gjort jobben sin i løpet av den tiden de har til rådighet.

Med bakgrunn i denne problemstillingen har derfor brukervennlighet be-

gynt å få et større fokus også i forskning og utvikling av sikkerhetssystemer.

Flere studier har begynt å adressere dette temaet i det siste. Blant annet et studie av Bardram viser problemene med innlogging godt [4]. I dette studiet ble det vist hvordan tradisjonelle løsninger for adgangskontroll som brukernavn og passord ikke passer inn i en hektisk hverdag på et sykehus. I en sykehussetting har en bruker behov for å logge seg på mange forskjellige systemer, på ulike enheter og gjerne mange ganger i løpet av en dag. Med bakgrunn i dette har Bardram utforsket og prøvd ut ulike alternative løsninger for innlogging med bra suksess. Mer detaljer om dette og andre lignende studier vil en finne i kapittelet relevant forskning. Andre studier [23] har også sett på problemet med å finne balansen mellom sikkerhet og brukervennlighet i en sykehussetting. Akkurat dette har Sapp (2004) sett nærmere på, selv om det ikke er med samme utgangspunkt som denne oppgaven, men med fokus på å finne mulige løsninger for "single sign-on". "Single sign-on" er en metode for å logge på flere systemer samtidig ved hjelp av en enkelt innlogging. Den største utfordringen ligger i at innloggingsrutinene i forskjellige systemer er bygget opp forskjellig og det er da en stor utfordring å få de til å "snakke samme språk" [23]

I studiet denne masteroppgaven omhandler vil jeg ta utgangspunkt i problematikken som beskrives over og i studier utført av Bardram og andre, og se hvordan dette problemet utfolder seg på St. Olavs Hospital i Trondheim. Ved å utføre intervjuer og observasjon av bruken av datasystemet og arbeidshverdagen til de ansatte ved sykehuset vil jeg ut ifra resultatene forhåpentligvis få rede på hvilke løsninger som passer best for deres situasjon, og ut i fra det foreslå endringer og eventuelt bruk av ny teknologi i dagens løsning.

1.1 Problemstilling

Dagens elektroniske pasientjournaler (EPJ) på sykehus krever relativt lang pålogging [12]. Dette fører til mye unødig arbeid ettersom leger og sykepleieres arbeid i stor grad er kjennetegnet ved mye avbrudd og mye mobilitet. Det er derfor ønskelig at brukeren lett skal kunne logge seg på og av forskjellige datasystemer. I dag skjer dette ved brukernavn og passord. Oppgaven går ut på å vurdere alternative metoder for autentisering slik som ID-kort, smartkort, fingeravtrykk, biometriske data, IButton [1] ring, stemme-ID. Oppgaven omfatter litteraturstudie, observasjon av og intervju med leger og sykepleiere, samt å foreslå krav og design for forskjellige autentiseringsmetoder i praktisk bruk.

Problemstillingen kan konkretiseres i følgende punkter:

- **Dagens praksis.**
  Det har fra flere hold, blant annet [12], blitt antydet at det er et problem med ugunstige løsninger og treg innlogging på sykehus. For å videre kunne utforske problemområdene med dagens praksis som har blitt antydet, så vil det bli utført observasjoner og intervjuer ved St.Olavs Hospital.

- **Krav til løsning.**
  Krav til løsninger for de identifiserte problemer vil bli utarbeidet med utgangspunkt i en analyse data fra observasjoner og intervjuer i kombinasjon med utforsking av relatert forskning og teori.

- **Egnethet av alternative teknologier.**
  Til slutt vil det bli gjort en utviklet et forslag til løsning som tilfredstiller kravene basert på sammenligning av teknologi som er egnet til formålet.

1.2 Studiets tilknytning til informatikkfaget

Dette studiet ligger mellom to tilsynelatende ulike forskningsfelt i informatikkfaget. På den ene siden er studiet relatert til fagområdet sikkerhet der hovedformålet er å studere mulige teknologier og tidligere studier. På den andre siden er fagområdene Systemutvikling og Menneske-Maskin Interaksjon, der viktigheten for god brukervennlighet spiller stor rolle i utviklingen av nye sikkerhetsløsninger. Men noe som denne oppgaven vil vise er at brukervennlighet og sikkerhet er derimot mer relatert til hverandre enn man skulle tro, da de gjensidig påvirker hverandre i utviklingen av et system. Dette kan forklares ved at et veldig sikkert system involverer komplekse sikkerhetsløsninger som gjør det vanskeligere for brukerne å utføre sine oppgaver, men på den andre siden hvis et system blir for enkelt kan det gå utover sikkerheten hvis systemet ikke inkluderer de passende sikkerhetsrutinene. Men som konklusjonene på slutten av denne oppgaven vil vise er sammenhengen ikke så enkel som det, disse konklusjonene vil forklare viktigheten av å inkludere brukeren som en del av systemet for å forstå brukerens viktige rolle som en viktig påvirkende faktor for sikkerheten.

1.3 Studiets plassering i systemutviklingsprosessen

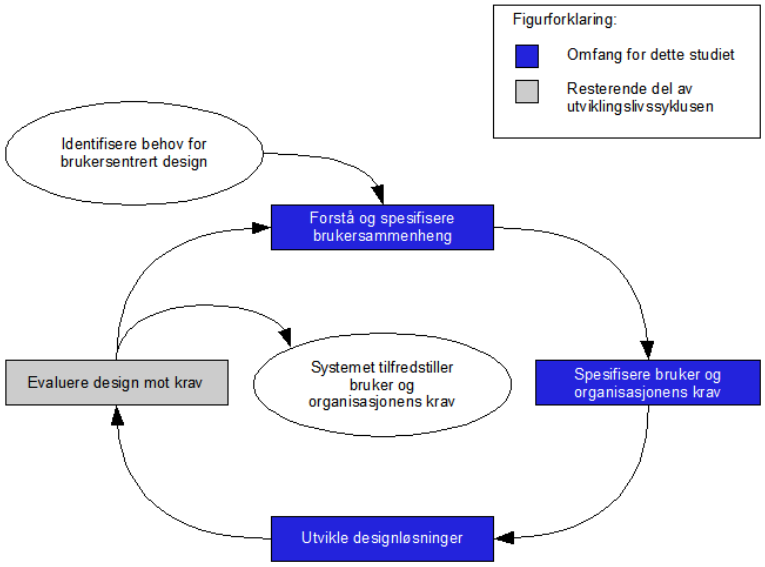
Dette studiets fokus er å utforske dagens praksis basert på observasjon og intervju, i tillegg til å foreslå alternative løsninger basert på teori og relatert forskning. Dette involverer å ta hensyn til brukere slik at en kan oppnå et system som er spesialtilpasset deres bruk og brukssammenheng. I en slik situasjon kreves utviklingsmetoder som setter brukerene i sentrum gjennom planlegging, design og utvikling av et produkt. En slik tilnærming til design blir kalt *brukersentrert design*. I en slik tilnærming er det informasjon om menneskene som vil bruke produktet som ligger til grunne for prosessen [19].

Den internasjonale standarden "ISO 13407: Human-centred design process" [14] er basis for mange brukersentrerte metodologier. Denne standaren definerer en generell prosess for ta i bruk brukersentrerte aktiviteter gjennom en utviklingslivssyklus. Modellen i figur 1.1 visualiserer denne standarden.

Denne figuren viser også hvilke deler av livsyklusen dette studiet har som omfang. Dette er vist i figur 1.1 ved at tre første stegene av modellen er uthevet med mørkere farge.

1.4 Studiets bidrag til forskningen

Det som er nytt med dette studiet er at få tidligere studier har gjort et så nøye studie før der sykehuspersonale ble følgt hver dag under observasjonene, ihvertfall ikke på St.Olavs hospital. Under observasjonene kommer en virkelig inn i hvordan de jobber, får sett og hørt om problemene og får et godt grunnlag for å finne nye forslag til nye løsninger som hjelper til med utviklingen av en kravspesifikasjon.



Figur 1.1: ISO 13407 med dette studiets omfang avmerket.

Kapittel 2

Innlogging

I dette kapitlet vil det bli sett nærmere på hva som menes med innlogging, hvilke metoder som finnes for innlogging og hvilke teknologier som blir brukt i sammenheng med innlogging. Med dette som bakgrunn vil det bli lettere å beskrive relatert forskning i senere kapitler.

Ifølge [7] er innlogging et forsøk på å få tilgang til et adgangskontrollert datasystem. Men ifølge den definisjonen sies det ikke at det er noe som kan skje bare ved å skrive inn et brukernavn og et passord. I sammenheng med datamaskiner har innlogging i de fleste systemer vært entydig med å skrive inn ett brukernavn og ett passord. Dette er noe som går tilbake til de tidligste "Mainframe[1] systemene" og senere systemer med operativsystemet UNIX[2]. De første mainframe maskinene hadde ikke innlogging, men senere når de fikk timesharing måtte jobber og brukere verifiseres. De tidligeste minidatamaskinene[3] hadde ingen innloggingsprosedyre, men med utbredelsen av UNIX på senere minimaskiner var innlogging nødvending[24]. Siden disse første systemene var kommando-baserte var tekstbasert innlogging naturlig. Men det finnes mange alternative metoder og teknologier for innlogging, og det er de som det skal sees nærmere på i denne oppgaven.

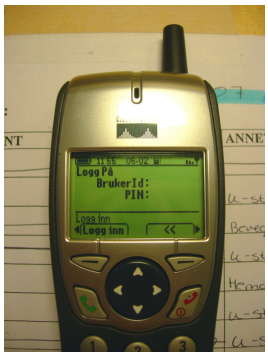
Hensikten med innloggingen i et system med adgangskontroll er å autentisere brukeren. I litteratur som angår tilgangskontroll er autentisering (eng. "authentication") det å verifisere identiteten til en bruker. Når det blir brukt i sammenheng med brukere som skal logge seg på et datasystem snakker man ofte om brukerautentisering (eng. "user authentication") [24]. Eksempler på

[1]Mainframe maskiner var andre generasjons datamaskiner i romstørrelse og var utbredt i 1955 og utover[24].

[2]UNIX er et av de første operativsystemene som ble utbredt på små datamaskiner. De var populære blant annet for sin mulighet for innlogging av flere brukere[24].

[3]Datamaskiner som var små nok til å stå på et arbeidsbord var regnet som minimaskiner.

(a) Leser for smartkort innebygget i tastaturet



(b) Cisco IP telefon med innlogging

(c) Kortleser med berøringsfri (RFID) teknologi i kombinasjon med PIN

Figur 2.1: Eksempler på moderne brukergrensesnitt for innlogging

moderne brukergrensesnitt for innlogging på sykehus er vist i figur 2.1(a), figur 2.1(b) og figur 2.1(c).

I mange tilfeller, spesielt på et sykehus, er det et behov for å autentisere en bruker i andre tilfeller enn når en bruker konkret logger på en datamaskin på tradisjonelt vis ved å skrive inn brukernavn og passord. Det kan være for eksempel når en bruker skal bli autentisert ved signering av en journal, ved åpning av låste dører eller når systemet vil dokumentere hvem som gjør hva [4]. I disse tilfellene blir det i følge definisjonen til Benantar ikke helt korrekt å bruke ordet innlogging siden man ikke snakker direkte om at en bruker prøver å få tilgang til et system. Ordet innlogging blir brukt i tittelen og introduksjonen på denne oppgaven. Dette er naturlig med tanke på at det er det som er mest brukt i dagligtale når man snakker om å få tilgang til et adgangskontrollert datasystem. Men videre vil autentisering bli brukt som en generelt term siden definisjonen på det er mer konkret og siden det er den termen som blir mest brukt i litteraturen. Autentisering vil bli gjennomgått i mer detalj i dette kapitlet.

2.1 Autentisering

Benantar (2006) definerer autentisering som sikker identifisering av en entitet, der en entitet er ”en aktiv agent som er i stand til initiere eller utføre en operasjon”. Det kan for eksempel være en bruker som kaller en kommando eller et program, en utførelsestråd eller en nettverksenhet. Benantar refererer også til autentisering som stadfesting av identitet. Da snakker en om

identiteten til en enhet, og om den enheten er den som den utgir seg for [7]. O'Gorman (2003) definerer dette ytterligere ved at han skiller mellom maskin-maskin autentisering ("maskin autentisering") og menneske-maskin autentisering ("bruker autentisering"). Ved maskin autentisering brukes veletablerte sikkerhets protokoller som er kjent for å være sikre. Et eksemplel er Secure Sockets Layer"(SSL) protokollen som brukes ved sikre transaksjoner på Internett. Men maskin autentisering bare bekrefter identiteten til maskinene og kan ikke si noe om identiten til brukeren ved maskinen. Dette er det brukerautentiseringen som skal gjøre [18], og det er denne form for autentisering som denne oppgaven har som fokus.

Stegene i autentiseringsprosessen

Autentisering er delt inn i forskjellige steg. Når man ser på disse får man en klarere forståelse hva autentisering omhandler. Inndelingen i de forskjellige stegene er i følge Bardram (2005):

1. Identifikasjon (eng. "Identification")
2. Verifisering/Stadfesting (eng. "Verification/Authentication")
3. Autorisasjon (eng. "Authorization")

I det første steget, *identifikasjon*, er hensikten å fastslå hvem brukeren er. Det andre steget, *verifikasjon/stadfesting*, skal verifisere at denne identiteten er det den utgir seg for å være. Den tredje og siste fasen, *autorisasjon*, har som mål å forsyne brukeren med korrekt tilgang til ressursen som den aktuelle brukeren har tillatelse til å bruke. Det skal også nevnes at noen også inkluderer *innrullering* (eng. "enrolment") som en første fase før de tre opplistet her. Denne fasen er som regel ikke regnet som en del av selve autentiseringen men som en første fase før brukeren kan bruke systemet for autentisering [25].

Tre typer autentisering

De ulike typene av metoder og teknologi for autentisering deles som regel inn i tre kategorier. Tradisjonelt har Bardram (2003) og andre [25] i litteraturen delt de ulike metodene inn i tre grupper. Disse er kategorisert som følger:

- Kunnskapsbaserte systemer: noe brukeren vet (for eksempel et passord)
- Tokenbaserte systemer: noe brukeren har (for eksempel et smartkort)
- Biometriske systemer: noe brukeren er (for eksempel fysiologiske trekk).

Andre [18] bruker en litt annerledes inndeling. O'Gorman (2003) har basert sin inndeling på den tradisjonelle tredelingen, men har brukt en litt annerledes terminologi. Han bruker termen "autentifikator" (eng. "authenticator") for det som blir brukt for å autentisere en bruker (for eksempel passord eller fingeravtrykk). Det som han refererer til som autentifikatore er egentlig de ulike typer av teknologier som finnes under hver type for autentiseringssystemer. Disse autentifikatorene grupperer han i tre kategorier. De tre typer av autentifikatorer deler han inn i:

- Kunnskapsbaserte autentifikatorer (det en vet)
- Objektbaserte autentifikatorer (det en har)
- ID-baserte autentifikatorer (hvem man er)

O'Gorman (2003) beholder den første kategorien, kunnskapsbasert, i sin terminologi slik som den tradisjonelt er brukt, mens han benytter kategorien objektbasert for det som tradisjonelt blir kalt tokenbasert, og han bruker ID-basert istedet for biometrisk. Han argumenterer for at den tradisjonelle oppdelingen ikke er uten problemer. For eksempel biometri er ikke hvem man er, det er bare en egenskap, og definerer en selv ikke noe mer enn hårfarge eller kroppsbygning gjør.

O'Gorman (2003) kategoriserer autentifikatorene etter hvordan de gir sikkerhet. En kunnskapsbasert autentifikator gir sikkerhet på bakgrunn av hemmelighet, for eksempel en kombinasjonslås eller et passord. En objektbasert autentifikator gir sikkerhet ved at den blir godt passet på og man har den nært inntil seg, for eksempel en metallnøkkel eller et minibankkort. En ID-basert autentifikator gir sikkerhet ved unikhet, for eksempel et pass eller biometri som er vanskelig å kopiere eller erstatte. Hver av kategoriene og autentifikatorene og eksempler på teknologi vil bli definert og utdypet mer senere i dette kapitlet.

Med bakgrunn av den klare definisjonen som O'Gorman bruker for kategoriseringen, er det denne inndelingen som vil bli brukt videre i denne oppgaven.

2.2 Ulike autentiseringsløsninger

De forskjellige typer av autentifiseringssystemer er her delt inn i O'Gormans tre kategorier. Hver type er definert og de forskjellige autentifikatorer er listet med eksempler på teknologier for hver av de. Et sikkerhetssystem består som

regel av flere typer autentifikatorer, men her listes de opp etter type autentifikator for å gjøre det mer oversiktlig. Kombinasjoner av autentifikatorer listes på slutten av dette kapitlet.

2.2.1 Kunnskapsbaserte sikkerhetsløsninger

Dette er systemer som tar i bruk autentifikatorer som blir ofte identifisert med "Noe en vet". Disse autentifikatorene karakteriseres ved at de er holdt hemmelig for andre. Eksempler på kunnskapsbaserte autentifikatorere er:

- **Passord.**
  Passord er single ord eller fraser som mer holdt hemmelig. Noen omtaler også personlige identifikasjons nummer (PIN). Hovedproblemet med passord er at et passord som er lett å huske er lett å gjette for utenforstående, og et langt, tilfeldig og randomisert eller skiftende passord er vanskelig å huske [18].

- **PIN.**
  Personlige identifikasjonsnummer (PIN) er i praksis det samme som passord, bare at det som regel blir brukt en kombinasjon av siffer med en lengde på vanligvis fire siffer. Disse har de lignende egenskapene og problemer som passord, som for eksempel at de kan bli gjettet og at en lang pinkode er lett å glemme. Men det er noen forskjeller, siden PIN-koder som regel er korte er problemet er ikke problemet så stort som med lange passord. O'Gorman (2003) omtaler PIN koder på samme måte som passord men i denne oppgaven blir de definert som en egen autentifikator siden de har litt andre egenskaper, som for ekspempel at de normalt tar kortere tid å taste inn, og kan i noen tilfeller være vanskeligere å huske [18].

2.2.2 Objektbaserte sikkerhetsløsninger

Objektbaserte autentifikatorer er de man kan forbinde med "det en har", disse er også blitt referert til som tokenbaserte autentifikatorer. Disse er karakterisert ved fysisk besittelse [18]. Denne kategorien inneholder objekter (eller "token" [4]) som for eksempel metallnøkler eller plastkort. For å skille mellom disse og kryptografiske nøkler brukes termen metallnøkler. For å vise ulemper og fordeler ved autentifikatorer innenfor denne kategorien kan en peke på et

[4]Av mangel på en god oversettelse av det engelske ordet "token", vil det her bli brukt som det er, altså token. I følge Merriam-Webster's Collegiate Dictionary [17] er token et karakteristisk trekk eller kjennemerke (eng. "a distinguishing feature".

eksempel fra O'Gorman (2003). En ulempe sikkerhetsmessig ved disse kan eksempelvis vises med tradisjonelle nøkler. Hvis man mister foreksempel en tradisjonell husnøkkel, så kan uvedkommende som har fått fatt i en nøkkelen komme seg inn i huset. Dette problemet gjelder også for digitale token, og det er derfor mange av de også er kombinert med et passord eller PIN kode. På den andre siden har objektbaserte autentifikatorer en klar fordel ved at hvis de er mistet oppdager eieren det og kan gjøre noe med det. Eksempler på objektbaserte autentifikatorer:

- **Metallnøkler.**
  Disse har i mange år gjort sin tjeneste som enkle og sikre autentifikatorer. Men i tillegg til sine klare fordeler har de som nevnt ovenfor også sine ulemper [18].

- **Nøkkelkort (for eksempel "Smartkort")**
  Nøkkelkort er kort (som regel plastkort) som kan brukes som en nøkkel til å få tilgang til for eksempel dører eller datasystemer. Hovedforskjellen mellom en tradisjonell metallnøkkel og nøkkelkort er at et nøkkelkort har en innebygget elektronisk signatur i forskjell til metallnøkler som har sin signatur i form av et unikt særpreg i utformingen. Noen nøkkelkort kan i tillegg til autentisering også brukes til identifikasjon [4]. Det som er felles for alle nøkkelkort er at de kan lagre informasjon.

  - *Hullkort*
    Den første typen nøkkelkort var *hullkortet*, VingCard [26], som ble oppfunnet av Tor Sørnes [5]. Dette var et plastkort med et mønster av hull for nøkkel som ble lest av en mekanisk dørlås.
  - *Magnetstripekort*
    Etterhvert fant også Tor Sørnes opp et elektronisk nøkkelkort med *magnetisk stripe* [20]. Dette er et kort som har en magnetisk stripe som inneholder informasjon, og er beregnet for å dra igjennom en kortleser.
  - *Kort med barkode*
    Andre kort har også informasjonen lagret i en *barkode* som er skrevet på kortet [11]. En barkode er en binær kode som utgjør et felt med stolper (eng. "bar") og mellomrom som skaper et mønster som kan bli tolket både numerisk og alfanumerisk. Dette mønsteret som representerer dataelementer og blir lest av en av en optisk leser[11].

[5] Historisk tidslinje for utviklingen av VingCard finnes på nettsiden http://www.vingcard.com/page?id=1561

- *Smartkort*
  I det siste er det en type nøkkelkort som har fått stor betydning og utbredelse, nemlig *smartkortet*. Smartkortet er et kort som kan ha databrikker av ulike typer innebygget og har dermed et bredt bruksområde. Som nevnt tidligere blir objektbaserte autentifikatorer ofte kombinert med passord eller PIN kode for å forbedre sikkerheten. Dette blir ofte gjort på blant annet smartkort, det kan man se ved systemer på for eksempel sykehus eller andre bygninger der et smartkort blir brukt sammen med en PIN kode [4].

Som en kan se fra de mange eksemplene av nøkkelkort ovenfor, finnes det mange måter å representere data på et kort, det er ofte bare snakk om å finne en teknologi som kan plasseres på et plastkort. En type teknologi som har fått spesiell betydning er *RFID*. RFID står for "Radio Frequency Identification" og er en elektronisk brikke som kan plasseres på blant annet et nøkkelkort [11].

- **RFID ("Radio Frequency Identification")** RFID teknologien har bredere bruksområde enn bare nøkkelkort og nevnes også her i et eget punkt. RFID-basert teknologi har blant annet blitt brukt for autentisering av personer ved RFID-implantat under huden [22], RFID-brikker innsydd i klær [8] og i pass [21]. I tillegg til RFID brukt i smartkort som nevnt ovenfor, kan RFID også brukes i

- **Kontaktbasert (for eksempel iButton)**
  En "iButton" [1] er en databrikke i liten (16mm tykk) stålbeholder som kan som kan bæres av en person eller en gjenstand. Denne brikken er liten nok til å kunne festes i en "key fob', en ring, en klokke eller en annen gjenstand, og kan bli brukt til adgangskontroll til bygninger og datamaskiner, og ulike dataloggingsoppgaver.

Digitale token

I den digitale verden er kryptografi et sentralt tema relatert til autentisering. For at passord og informasjon om brukeren ikke skal komme på avveie når autentifiseringsgjenstander blir brukt må slik informasjon krypteres ved hjelp av kryptografiske algoritmer. For å kryptere og dekryptere informasjon bruker en *kryptografiske nøkler*. Kryptografiske nøkler (eng. Cryptografic keys) er digitale i forskjell til sine håndfaste fysiske motstykker. Kryptografiske nøkler blir implementert av kryptografiske algoritmer. Disse algoritmene kan klassifiseres på flere måter, en måte er å klassifisere de etter antallet av nøkler som

er tatt i bruk for kryptering og dekryptering. Kessler (1998) har klassifisert de tre typene av algoritmer slik:

- *Secret Key Cryptography (SKC)*: Bruker en enkel nøkkel for både kryptering og dekryptering
- *Public Key Cryptography (PKC)*: Bruker en nøkkel for kryptering og en annen nøkkel dekryptering
- *Hash funksjoner*: Bruker en matematisk transformasjon for å kryptere informasjon irreversibelt

Mer detaljert informasjon om kryptografi finnes i [15] og [16]

2.2.3 ID-baserte sikkerhetsløsninger

Dette er sikkerhetssystem som er basert på autentifikatorer som blir assosiert med "noe en er". O'Gorman (2003) bruker som nevnt over kategorien ID-basert [18] i forhold til kategorien biometrisk [4]. Forskjellen her er at ID-basert i tillegg til å inkludere biometriske autentifikatorer også inkluderer andre autentifikatorer som unikt identifiserer en person, som for eksempel førerkort eller pass. O'Gorman (2003) omgår spørsmålet om at en biometri har er unikt i den forstand at der finnes kun en i verden, og heller hevder at det er distinktivt til den grad at det er høyst usannsynlig at to biomtriske autentifikatorer vil være helt like, i alle fall for det enkelte system. En biometri er som et et nummer på et førerkort, det er ikke hemmeligheten av nummeret som gjør det sikkert, det er vanskeligheten med å etterligne originalen som gjør det til en god autentifikator [18]. Eksempler på ID-baserte autentifikatorer fra [18] er:
Biometriske:

- **Fingeravtrykk** - Stabilt biometrisk signal
- **Ansikt** - Stabilt biometrisk signal
- **Hånd** - Stabilt biometrisk signal
- **Iris** - Stabilt biometrisk signal
- **Retina** - Stabilt biometrisk signal
- **Stemme** - Foranderlig biometrisk signal
- **Gange** - Foranderlig biometrisk signal

- **Tastemønster (eng. "Keystroke")** - Foranderlig biometrisk signal [3]

Andre:

- **Førerkort**
- **Pass**
- **Bankkort (med bilde)**

2.2.4 Kombinasjonsløsninger

Visse autentifikatorer kan også kombineres for å forbedre sikkerheten. Dette blir kalt flerfaktor autentisering (eng. "multifactor authentication". Da må man være sikker på at begge autentifikatorene er sikre, forholdsregler for sikkerheten som blir tatt her er da at en Boolean AND operasjon blir utført for hver autentifikator til hver faktor sine autentiseringsresultater til alle er bekreftet [18]. Kombinasjonsløsninger kan være:

- **Smartkort med PIN**
- **Biometri med passord**

Kombinasjon med for eksempel et bankkort og en PIN-kode (to-faktor autentisering) gir fordelen at et kort kan mistes, men med en PIN-kode gir dette ekstra sikkerhet siden andre enn eieren ikke kan bruke kortet uten å vite koden [18]

2.3 Sammenligning av autentiseringsløsninger

Metoder for sammenligning av autentiseringsmetoder og autentiseringsteknologi blir i sikkerheten ofte målt i forhold til effektivitet og hvor god krypteringen er. Blant annet blir false-acceptance-rate (FAR) brukt for å måle sannsynligheten for at systemet feilaktig erklærer en suksessfull treff mellom inndata mønsteret og et ikke-matchende mønster i databasen. False-rejection-rate (FRR) er sannsynligheten for at systemet feilaktig bestemmer et feil i treff mellom inndata mønsteret og den matchende malen i databasen.

Kapittel 3

Relatert forskning

Forskning som er relatert til temaet i denne masteroppgaven kommer fra flere ulike typer av forskningsdisipliner. Det er både forskning innenfor teknologi for adgangskontroll, utvikling av enheter og systemer som tar i bruk slik teknologi, forskning som går på evaluering av brukbarheten av teknologien eller enheter som tar i bruk teknologien, og også forskning direkte rettet mot innloggingsproblematikken, da både på sykehus og andre institusjoner.

Forskning innenfor adgangskontroll har tatt seg opp siste årene da sikkerhet har blitt enda viktigere i dagens digitale verden, og i tillegg på grunn av at teknologi og løsninger for adgangskontroll har blitt mer utviklet og tatt i bruk. Spesielt fremskritt innenfor biometri og trådløs dataoverføring har gjort dette mulig.

3.1 Brukervennlighet vs. Sikkerhet

I kapittel 1.2 ble sammenhengen mellom brukervennlighet og sikkerhet introdusert. Dette er et to områder som krever stor oppmerksomhet når det utvikles systemer som krever høy sikkerhet og som samtidig vedrører brukere. Dette er ikke aktuelt bare på sykehus, men også i alle andre sikkerhetsrelaterte systemer som brukere samhandler med. Dette har ikke vært to temaer som man har tidligere oppfattet som relaterte men som i det siste årene begynt å få litt mer oppmerksomhet. Blant annet har interdisiplinære forskere og andre innenfor menneske-maskin interaksjon, sikkerhet og personvern kommet i sammen og dannet konferansen "Symposium On Usable Privacy and Security" (SOUPS)[1]. Den første konferansen ble holdt i 2005 i Pittsburg, Pennsylvania. Her har også temaer innenfor brukerautentisering

[1]SOUPS er sponset av Carnegie Mellom CyLab, og nettsiden for konferansen kan nåes på: `http://cups.cs.cmu.edu/soups/`

blitt diskutert. En artikkel som har blitt publisert i sammenheng med denne konferansen er [10]. Denne artikkelen beskriver et brukbarhetsstudie som ble gjort av programvaren "Polaris". Dette er en programvare for å hindre virus i å forandre filer, og var designet for å stille brukervennlighet på side med sikkerhet. Dette studiet viste at tross i at programmet var designet med vekt både på sikkerhet og brukervennlighet, så hadde det problem med at brukere omgikk sikkerheten til fordel for å heller få gjort arbeidet raskere. Forfatterne poengterte også problemet med at når brukervennligheten er lagt til i etterkant av et ferdig system i forhold til å inkludere det fra starten av. Forfatterne avsluttet med tre råd. For det første må en redusere tilfeller der brukerne har ansvar med å gjøre sikkerhetsrelaterte valg. I tillegg kan en motvirke tilfeller der sikkerheten omgås ved å sørge for det er den raske måten å gjøre ting på som er den sikre. Til slutt kan er en integrering av sikkerhetsløsninger i operativsystemet gjennom utvikling. En annen artikkel [9] tar for seg lignende problematikk og kommer frem til litt av de samme konklusjonene, men er litt annerledes enn andre studier ved at de tar utgangspunkt i hvordan sikkerheten selv kan manifistere seg som en del av brukernes samhandling med informasjonssystemer. Her ser de på hvordan brukere opplever og tolker sikkerhetssituasjoner, og hvordan de blir enten hemmet eller gjort i stand ved hjelp av eksisterende løsninger til å håndtere situasjonen på en sikker måte.

I [25] blir det gjort en evaluering av biometriske verifikasjonsystemer. Her er det gjort en sammenligning med bakgrunn i ISO 9241-11 [2] der de tar for seg disse tre aspektene:

- "Effectiveness"
- "Efficiency"
- "Satisfaction"

Andre har også gjort sammenligninger av forskjellige autentiseringssystem for å vise deres fordeler og ulemper. Blant annet i [7] vises en tabell for en slik sammenligning. Denne tabellen er vist i figur 3.1.

3.2 Sikkerhet på sykehus

Det blir også blitt gjort forskning direkte rettet mot innloggingsproblematikken på sykehus, der en prøver å finne løsninger på problemet med at innloggingsløsninger ikke er tilpasset den hektiske hverdagen på sykehus. For eksempel i Danmark er det et pågående prosjekt [4] innenfor dette temaet

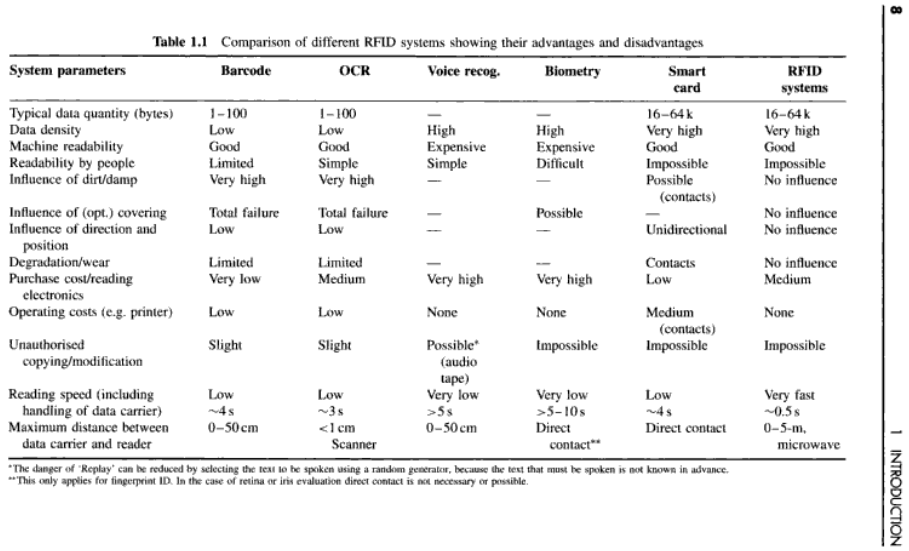


Table 1.1 Comparison of different RFID systems showing their advantages and disadvantages

System parameters	Barcode	OCR	Voice recog.	Biometry	Smart card	RFID systems
Typical data quantity (bytes)	1–100	1–100	—	—	16–64 k	16–64 k
Data density	Low	Low	High	High	Very high	Very high
Machine readability	Good	Good	Expensive	Expensive	Good	Good
Readability by people	Limited	Simple	Simple	Difficult	Impossible	Impossible
Influence of dirt/damp	Very high	Very high	—	—	Possible (contacts)	No influence
Influence of (opt.) covering	Total failure	Total failure	—	Possible	—	No influence
Influence of direction and position	Low	Low	—	—	Unidirectional	No influence
Degradation/wear	Limited	Limited	—	—	Contacts	No influence
Purchase cost/reading electronics	Very low	Medium	Very high	Very high	Low	Medium
Operating costs (e.g. printer)	Low	Low	None	None	Medium (contacts)	None
Unauthorised copying/modification	Slight	Slight	Possible* (audio tape)	Impossible	Impossible	Impossible
Reading speed (including handling of data carrier)	Low ~4 s	Low ~3 s	Very low >5 s	Very low >5–10 s	Low ~4 s	Very fast ~0.5 s
Maximum distance between data carrier and reader	0–50 cm	<1 cm Scanner	0–50 cm	Direct contact**	Direct contact	0–5-m, microwave

*The danger of 'Replay' can be reduced by selecting the text to be spoken using a random generator, because the text that must be spoken is not known in advance.
**This only applies for fingerprint ID. In the case of retina or iris evaluation direct contact is not necessary or possible.

Figur 3.1: Sammenligning av ulike RFID systemer fra [7]

på sykehus). I dette studiet ble det gjort feltstudier på et sykehus for å avdekke brukbarhetsproblemer med innloggingsprosedyrene. Her ble det gjort observasjoner og intervjuer av leger og sykepleiere. Resultatene av dette studiet avdekket at sikkerhetsrutiner og innloggingsprosedyrer ble omgått på grunn av tungvinte løsninger. Sikkerhetsbrudd var for eksempel at det skrevet ned passord direkte på skjermer, man "lånte" innlogging hos andre og man skrev ned passord eller gjorde de enkle å huske. De ansatte forandret også sin daglige rutine for å omgå innlogging. Men dette ble gjort på grunn av at man ville få arbeidet gjort fortere. Man fant også nye rutiner på daglige gjøremål for å slippe å logge inn. Før elektronisk journal og innlogging ble innført hadde man en enkel rute å gå for å for eksempel levere ut medisin. Nå måtte man inn på en datamaskin både før og etter en hadde levert medisin til pasienten på rommet, og sykepleierne fant da ut nye rutiner for å slippe unødvendig innlogginer. En rutine for dette var å skrive ut informasjon på papir om morgenen så man skulle slippe å gå inn på en datamaskin hver gang utover dagen. Etter endt arbeidsdag ville man gå inn på en datamaskin og skrive inn informasjonen man hadde samlet i løpet av dagen. Dette er ikke slik systemet var designet, og i tillegg til at det medførte brudd på sikkerhetsrutiner ble også en del av oppsporingsmulighetene for hvem som gjør hva mistet. Etter observasjoner på sykehuset designet forskningsgruppen nye mekanismer for autentisering. I utviklingen av disse satte de stor vekt på nærhetbasert bruker verifikasjon, stille innlogging, vandrende bruker

sesjoner, og hvilende sesjoner.

Andre studier har sett på muligheten for å kontrollere tilgang til brukere ved å innføre et lokasjonssystem. Der brukeren blir registrert ved ulike steder i bygningen ved hjelp av trådløse mottakere og sendere med RFID baserte teknologi. Systemet bruker da dette systemet til å fastslå om det er fysisk mulig for å en bruker å få tilgang til et sted hvis han ble nettopp registrert et annet sted.

Et studie har også sett på bruken av Smart-telefoner til å kontrollerere tilgangskontroll [6]. Her ble det sertifikater registrert på telefonen, og man kunne bruke den til å få tilgang til visse ressurser. Hvis en bruker hadde behov for å midlertidig "låne" innlogging hos en annen bruker, kunne informasjon om dette bli sendt fra en telefonenhet til en annen.

Kapittel 4

Forskningsmetode generelt

Forutsetninger for grunnforskning og anvendt forskning Hvor går grensene for det vi vet i dag, og hvilke muligheter har vi for å finne ut noe vi ikke vet fra før? Hvordan kan vi gjennom å anvende tilgjengelige metoder finne ut noe vi ikke vet fra før? [13] ..mer her

4.1 Systemutvikling

Systemutvikling er et forskningsfelt som. ..mer om generelle modeller og metoder

4.2 Brukervennlighet

I introduksjonen ble viktigheten med brukervennliget nevnt og ISO 13407 standarden ble introdusert sammen med dens relevans til dette studiet. Denne standarden er er generell tilnærming til brukersentrert design, men som nevnt før spesifiserer den ikke spesifikke metoder [14]. Metoder og retningslinjer som er relevante til dette studiet er blant annet observasjonsteknikker, protyping og testing.

4.3 Intervju

Ulike typer:
- Str.
- Sen.

4.4 Observasjon

Under

4.5 Prototyping og testing

Prototyping er et første steg av implementeringen mot et ferdig produkt. Dette er viktig for å finne ut hvilke løsninger vil la seg praktisk gjennomføre. I tillegg er tidlig testing viktig, og derfor er det viktig å få på plass en prototype som kan brukes til testing [19] Omfanget for denne oppgaven omhandler ikke utvikling av prototype, men prototyping av foreslåtte løsninger vil bli det neste steget i utviklingsprosessen i forhold til hva som er blitt gjort i dette studiet.

Kapittel 5

Metodevalg

Dette kapitlet vil beskrive valg av metode, samt beskrive hva den valgte metode innebærer, og tilslutt utdype hvordan metoden ble gjennomført i dette studiet.

5.1 Forskningsdesign

På et sykehus jobber det folk fra mange forskjellige yrkesgrupper, og innad i de ulike yrkesgruppene er det også en bred alderspredning. Dette gjør at de ansatte har veldig ulik bakgrunn og ulike arbeidsoppgaver. Dette gjør det viktig å velge en metode som så korrekt som mulig kan fastslå arbeidssituasjonen som brukerne av systemet befinner seg i.

For å kunne få en mest mulig reell beskrivelse av arbeidssituasjonen til de ansatte ved sykehuset valgte jeg observasjon som metode. Ved å involvere meg direkte i deres hverdag og observere arbeidsrutiner kunne jeg få et veldig godt inntrykk av hvilke behov de har. Observasjon ville gi meg et objektivt inntrykk siden jeg var en utenforstående som satte meg inn i deres situasjon.

I tillegg valgte jeg også å intervjue de ansatte så jeg kunne få subjektive meninger om hva de synes om systemet. Ved å bruke både observasjoner og intervju kan jeg sammenligne resultatene fra de to metodene. Gangen i studiet:

1. Litteraturstudie

2. Forstudie (planlegging / kort finne ut hva som blir gjort på sykehuset nå)

3. Observasjon (nøye observasjon og kartlegging av bruksvaner og problematikk)

4. Intervju med leger og sykepleiere
5. Analyse
    - Kvalitativ
    - Kvantitativ (statistikk)

5.2 Observasjon

Her vil en beskrivelse på hva jeg ville komme frem til og hvilke midler jeg tok i bruk for å finne det ut. Om observasjonene og hva jeg gjorde, hvordan jeg gjorde det, hva jeg ville finne ut, hvordan det fungerte ved å gjøre det slik jeg gjorde.

Observasjonene ble utført på St.Olavs hospital i Trondheim i en periode over tre uker i januar og februar 2008. Her ble det i hovedsak observert på Nevrologisk Sengepost i Nevrobygget der det jobber i hovedsak sykepleiere, hjelpepleiere og leger.

Observasjonene ble gjennomført i hele dager der tidspunkt for pålogging ble registrert, hvem som logget på, hva programmer som ble brukt, hva innloggingstiden var, og om det ble registrert noe spesielle problemer under påloggingen. Det ble også spurt spørsmål om systemet under observasjonene, men ikke så det forstyrret brukerene.

Alle data ble registrert på loggark og i notater, som senere ble skrevet elektronisk og analysert.

Bevegelsesmønstret til de ansatte ble også registrert. Dette ble registrert ved linjer som representerte bevegelse, disse ble registrert på et kart over avdelingen for å avdekke bevegelsesmønstret til en ansatt.

Hovedformålet med observasjonene var å avdekke problemområder i tillegg til å finne ut hvilke behov de ansatte har for tilgang til systemet. Dette vil kunne hjelpe i vurderingen for nye løsninger.

5.3 Intervju

Intervjuene ble utført på samme avdeling som observasjonene. Det ble utført ett pilotintervju for å luke ut eventuelle urelevante spørsmål. Etter en liten redesign av intervjuet ble 20 intervjuobjekter intervjuet.

Intervjuobjektene var leger, sykepleiere og hjelpepleiere.

Intervjuene ble tatt opp på lydbånd, og i den sammenheng ble et samtykkeskjema skrevet under av hver deltaker.

5.4 Statistikk

Alle dataene som ble registrert i tabellform for at de skulle lettere analyseres og slik at man kunne produsere statistikk.

Kapittel 6

Resultat fra observasjon og intervju

De innsamlede data er fra observasjoner og intervjuer på en avdeling på et sykehus. Generaliserbarheten av disse dataene for andre avdelinger og sykehus kan i dette tidspunkt ikke fastslås med sikkerhet og i detalj, men vi ser noen trekk som går igjen med andre studier, som for eksempel i [5]. Studiet ble som nevnt i introduksjonen utført på Nevrologisk avdeling ved St.Olavs Hospital. Første del beskriver dagens situasjon ved dagens system i tillegg til en beskrivelse av avdelingen og dens brukere. Videre vil det bli gitt en oppsummering av innsamlede data fra både observasjoner og intervjuer. Både observasjonene og intervjuene var todelt. De bestod begge av både en kvantitativ del og en kvalitativ del. Resultatet fra innsamlingen av begge disse vil bli gjennomgått i detalj i dette kapitlet.

6.1 Dagens situasjon

I dagens situasjon på St.Olavs hospital har, det som nevnt i introduksjonen, at det er et ønske om forbedring av svakheter ved dagens system. Det har blitt rapportert [12] at det oppleves flaskehalser i arbeidsflyten på grunn av tungvindte løsninger. Dette har i dette studiet blitt gransket nærmere. Faktorene som er tatt i betraktning under denne granskningen er:

- Sikkerhet - Sikkerhet er viktig både for å hindre adgang til lukkede systemer og til å sikre dokumentasjon.

- Brukervennlighet - Brukervennlighet er viktig for å oppnå et effektivt system som er med på å opprettholde sikkerheten.

- Andre faktorer - For eksempel praktiske faktorer i henhold til aktuell teknologi.

Før hovedresultatene av observasjonene og intervju blir presentert vil det bli gitt en kort beskrivelse av avdelingen for å få et bedre innblikk i deres hverdag. Informasjonen om avdelingen ble tilegnet under observasjonene.

6.1.1 Beskrivelse av avdelingen

Avdelingen som observasjonene ble utført på er en Nevrologisk sengepost. Denne avdelingen består av tre "tun". De sykepleierne, hjelpepleierne og legene som er jobber der har ansvar for alle de tre tunene. Hvert tun består av pasientrom med senger, lagerrom, toaletter og undersøkelsesrom. Hvert tun har også et lite område med datamaskiner hvor ansatte kan få tilgang til datasystemet med elektroniske pasientjournaler. Avdelingen har også en stue/matsal for pasientene, pauserom for de ansatte. Ellers er det også et medisinrom på avdelingen med en datamaskin og et felleskontor med datamaskiner. Undersøkelsesrommet har tre datamaskiner, dette rommet blir mest brukt til morgenmøte, rapportmøte ved vaktskifte og møte i sammenheng med pasientrunden.

En typisk dagvakt starter med et besøk i garderoben for å ta ut tøy før de går opp på avdelingen. Det første de gjør er å starte med et morgenmøte. På morgenmøte går de sykepleierne og hjelpepleierne som er på dagskiftet gjennom pasientlisten og hva som skal skje utover dagen. Her er gruppeleder pålogget en maskin med DocuLive oppe der hun har pasientoversikten foran seg. De andre følger med og noterer på sin pasientliste som er skrevet ut på et papir. Dette papiret med pasientoversikten brukes utover dagen. Etterhvert utover dagen går med til stell og pleie til pasientene. Utlevering av mat og medisiner. Hvis en pasient skal til en undersøkelse (for eksempel røntgen) blir pasienten trillet til den avdelingen undersøkelsen skal være. Ved uttak av medisiner tar sykepleierne ut medisin på medisinrommet, til medisinrommet kreves det at kort brukes. Her er det sykepleierne som har adgang. I ti-tiden går legene en runde innom alle pasientene sammen med sykepleiere forå å sjekke pasientens tilstand i tillegg til å informere pasienten om nye utviklinger. Legene bruker ikke datamaskinen på rommet til pasientene, men forbereder seg på forhånd og har med seg all informasjon de trenger i papirform. I etterkant av denne runden logger de ofte inn på en datamaskin som står i avdelingen for å skrive notater eller hente informasjon. En halvtime før vaktskifte har det avtroppende vaktskiftet rapportmøte, der går de igjennom vakten som har vært og diskuterer pasientene.

6.1.2 Innloggingsrutine

For å logge inn i systemet er det mange steg før man får tilgang til den ressursen man ønsker. Stegene for logge seg på blant annet DocuLive er som følger:

1. Først innlogging til Windows med kort i smartkortleser og taste inn PIN kode (mellom 30 sekunder og ett minutt)
2. Vent på at Windows lastes inn og dine innstillinger lastes
3. Vent på at Kilden åpner seg (Internet Explorer åpnes som standard med Kilden som startside)
4. Gå til startmenyen og finn DocuLive under programmer i startmenyen
5. Vent på at innloggingsvindu for DocuLive skal lastes (30 sekunder)
6. Skriv inn brukernavn og passord og trykk Enter eller klikk med OK med mus
7. Vent på at DocuLive skal åpne seg (30 sekunder)

Ved utlogging kan en enten lukke alle vinduer og systemer en har oppe, og så trykke Logg ut fra startmenyen i Windows, for så å dra ut kortet. Eller en kan bare dra kortet rett ut mens en har oppe alle systemene. Ved ny innlogging er da tanken at man skal kunne komme inn til samme sesjon der en avsluttet med systemene fortsatt oppe. Dette fungerer bare i noen tilfeller, hvilke tilfeller er uklart.

DocuLive er ett av mange systemer sykepleierne, hjelpepleierne og legene på avdelingen bruker. I tillegg finnes det mange ulike systemer som de må logge seg på for å gjøre sine daglige gjøremål. En oversikt over dette vil en finne i delen om resultater fra intervjuer i kapittel 6.3.

Videre i dette kapittelet vil det bli gitt en oppsummering av de data som ble samlet inn av observasjonene og intervjuene, både kvalitative og kvantitative data. Dette vil gi et bilde av bruksmønster hos brukerne og et bilde av brukbarheten og effektiviteten ved systemet.

6.2 Resultat fra observasjon

Denne delen vil oppsummere resultater fra observasjonene. Både i form av kvantitative resultater fra de strukturerte observasjonene som viser målinger av innloggingstid, antall innlogginger og brukshyppighet for ulike systemer. I tillegg vil også kvalitative resultater fra den ustrukturerte observasjonen presenteres.

6.2.1 Kvantitative resultater fra observasjon

Observasjonene ble utført av en observant i en periode på tre uker. Observasjonene gikk over hele dager, ett arbeidsskift fra kl.08:00 til kl.15:00. De første dagene ble det i tillegg til kvantitative målinger også gjort observasjoner av hvordan systemet og avdelingen fungerte i praksis. Kvalitative data ble også samlet inn. Dette ble samlet inn i form av notater fra observasjoner av hvordan brukerne utførte oppgavene sine, hvilke problemer som oppsto, hvordan brukerne taklet slike situasjoner og hvordan systemet taklet problematiske situasjoner. Spørsmål ble også stilt til brukerne når det passet seg slik at det ikke virket forstyrrende.

Før målingene presenteres vil en forklaring av de innsamlede data gis. Det som ble observert og registrert var følgende:

- **Innloggingstid.** Tid målt fra det øyeblikk setter seg ned eller stiller seg foran skjermen for å logge inn, til brukeren har fått logget seg inn på et undersystem/program.

- **Total tid innlogget per innlogging.** Dette er tiden fra brukeren starter innloggingen til han/hun logger ut og drar ut kortet. Tiden systemet bruker på å avslutte sesjonen etter at brukeren har valgt å logge ut er ikke tatt med, dette er ikke med i del interaksjonen med brukeren har med systemet, i de fleste tilfeller går brukeren ifra systemet også etter at han/hun har initiert utloggingen ved å for eksempel trykke på logg ut i Windows eller drar ut kortet direkte.

- **Går ifra åpen sesjon og personlig smartkort.** Registrert hvis bruker gikk bort fra maskinen mens hun/han var innlogget og lot kortet stå igjen og sesjonen åpen.

- **Usuksessfulle eller avbrutte innlogginger.** Hvis bruker ikke fikk logget inn eller innloggingen ble avbrutt.

Data for observasjonene følger i delkapitlene under. Her oppsummeres hver del og data er vist i tabellform og grafisk i tillegg til tekstlig.

De kvantitative målingene ble utført ved at hver innlogging ble registrert i en observasjonslogg. Her ble det blant annet registrert tid. De fleste målingene av innloggingstid på datamaskin ble gjort med vanlig klokke, men på slutten ble de siste 28 målingene gjort nøyaktig med stoppeklokke. Fordelen med det er klar, men bakdelen av det ble at man ikke fikk registrert andre hendelser på avdelingen og man fikk ikke registrert alle innlogginger på alle maskinenene på avdelingen.

Innloggingstid

Det ble totalt registrert 100 innlogginger, dette inkluderte 97 innlogginger på datamaskin, 2 bruk av rørpost og 1 pålogging av telefon. Grunnen til at det var så få registreringer av rørpost og telefon var at de kvantitative målingene skulle i hovedsak omhandle innlogging på datamaskin. Utifra de 97 innlogginger på datamaskin var det 87 målinger der tiden det tok for innlogging ble registrert. Det er disse 87 som blir brukt for statistikk på innloggingstid. Grunnen til at ikke alle målinger ble registrert med innloggingstid var at siden det var bare en observatør kunne han ikke holde oversikt over alle maskinene på avdelingen samtidig, og noen ganger ble en pålogging begynt før han fikk tid til å se på klokka før innloggingen startet, men denne innloggingen ble registrert likevel i det øyemed at andre data som antall ganger brukeren gikk fra maskinen kunne bli registrert, eller andre observasjoner i kvalitativ form kunne bli registrert.

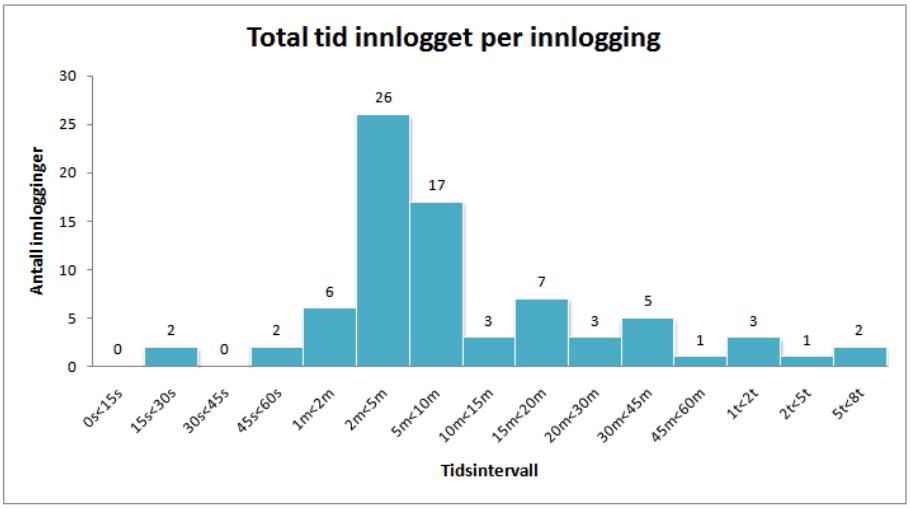
Av de 87 påloggingene som ble registrert med innloggingstid ble ble en gjennomsnittlig innloggingstid utregnet til 1 minutt og 11 sekunder. For kontroll var gjennomsnittlig innloggingstid der det ble brukt stoppeklokke 1 minutt og 21 sekunder. Dette ble regnet utifra totalt 23 som det ble registert tid for.

Antall påloggingen av de 87 registrerte med tida var det totalt 16 som hadde en innloggingstid $\geq$ 2 minutt. I prosent av de 87 blir dette 18,39 %.

Tid innlogget per innlogging

Gjennomsnittlig tid en bruker var innlogget en datamaskin under en enkelt innlogging ble registrert ut fra 87 innlogginger. Total tid innlogget per innlogging er hvor lenge totalt sett en bruker var innlogget en maskin, sett bortifra spørsmålet om brukeren gikk i fra maskinen eller ikke mens hun/han var innlogget. Her ble gjennomsnittlig tid 22 minutter. Dette kan være i overkant av vanlig bruk, på grunn av at noen få av innloggingene var ekstra lange (opptil flere timer) og dette kan ha påvirket gjennomsnittstiden. Antall tider foran en datamaskin som var registrert med mer enn en time var 5 innlogginger, altså 5,75 % av de 87 innloggingene som var registrert med tid. Fordelingen av antall innlogginger fordelt på de ulike tidsintervaller er vist i figur 6.1

For kontroll ble det registert 23 innlogginger med stoppeklokke. Disse ble gjort kun på datamaskiner som ble brukt ute i det åpne landskapet i avdelingen og ikke på undersøkelsesrommet eller på maskinen til postsekretæren. Disse målingene gav en gjennomsnittstid på 16 minutter og 1 sekund. Dette viser at den første gjennomsnittstiden som ble utregnet var litt i overkant (5 minutter og 91 sekund mer enn kontroll med stoppeklokke) på grunn av



Figur 6.1: Fordelingen av tid innlogget over tidsintervaller

noen få innlogginger med ekstra lang innloggingstid.

Går ifra åpen sesjon og personlig smartkort

Noe som var et vanlig fenomen under observasjonene var at brukere gikk ifra datamaskinen hvor de var innlogget uten å logge ut eller ta med seg kortet. Da ble sesjonen stående åpen med sensitiv informasjon tilgjengelig for tilfeldig forbipasserende, og det personlige smartkortet ble stående igjen i datamaskinen. Ved 23 av de 97 registrerte innlogginger på datamaskin gikk brukeren fra maskinen med kortet i og sesjonen fortsatt åpen. Dette tilsvarer en prosentandel på 23,71 % av de 97 påloggingene.

Brukere gikk også ifra maskinen flere ganger under en pålogging. For hvert innlogging ble det registret hvor mange ganger en bruker gikk ifra maskinen med kortet stående i. Gjennomsnittet for hvor mange ganger en bruker gikk ifra var 2,05 ganger per innlogging.

I 14 av innloggingene ble tiden en bruker gikk i fra maskinen også registrert. For disse 14 innloggingene var det totalt 27 tilfeller hvor en bruker gikk i fra maskinen (en bruker går ofte i fra maskinen flere ganger under en innlogging). Gjennomsnittet for hvor den totale tiden en bruker gikk ifra maskinen under en innlogging var 8 minutter og 34 sekunder. Den gjennomsnittlige tiden en bruker gikk i fra maskinen regnet ut i fra de 27 enkelttilfellene var 4 minutt og 26 sekunder. Det lengste en bruker gikk ifra var 1 time, men dette ene tilfelle med en time var mye lengre enn de andre som lå mellom 10 minutt og 25 sekund. Her er standardavviket regnet ut. Standardavviket

ble $\sigma = 666$ sekunder. Dette gjort om til minutt blir 11 minutt og 6 sekund. Tiden en bruker går i fra på fordelt på de 27 tilfellene er vist i figur 6.2.

Usuksessfulle innlogginger

Noe som også ble registrert var antall usuksessfulle innlogginger og avbrutte innlogginger. Usuksessfulle innlogginger var innlogginger der brukeren satte i kortet og forsøkte å logge seg på, men av en eller annen grunn ikke fikk tilgang til systemet. De steder eller tilfeller hvor det ble registrert ved observasjonene at en bruker ikke fikk logget seg inn listes opp nedenfor. Det er også andre steder eller tilfeller der brukere ikke fikk logget seg inn eller ikke ble autentisert på annet vis, men det er ikke med i denne statistikken. Grunnen til det er at dette var tilfeller som kom frem under intervjuene eller under samtaler med brukere under observasjonen, og her ble det ikke registrert statistikk, dette vil bli utdypet senere i oppgaven.

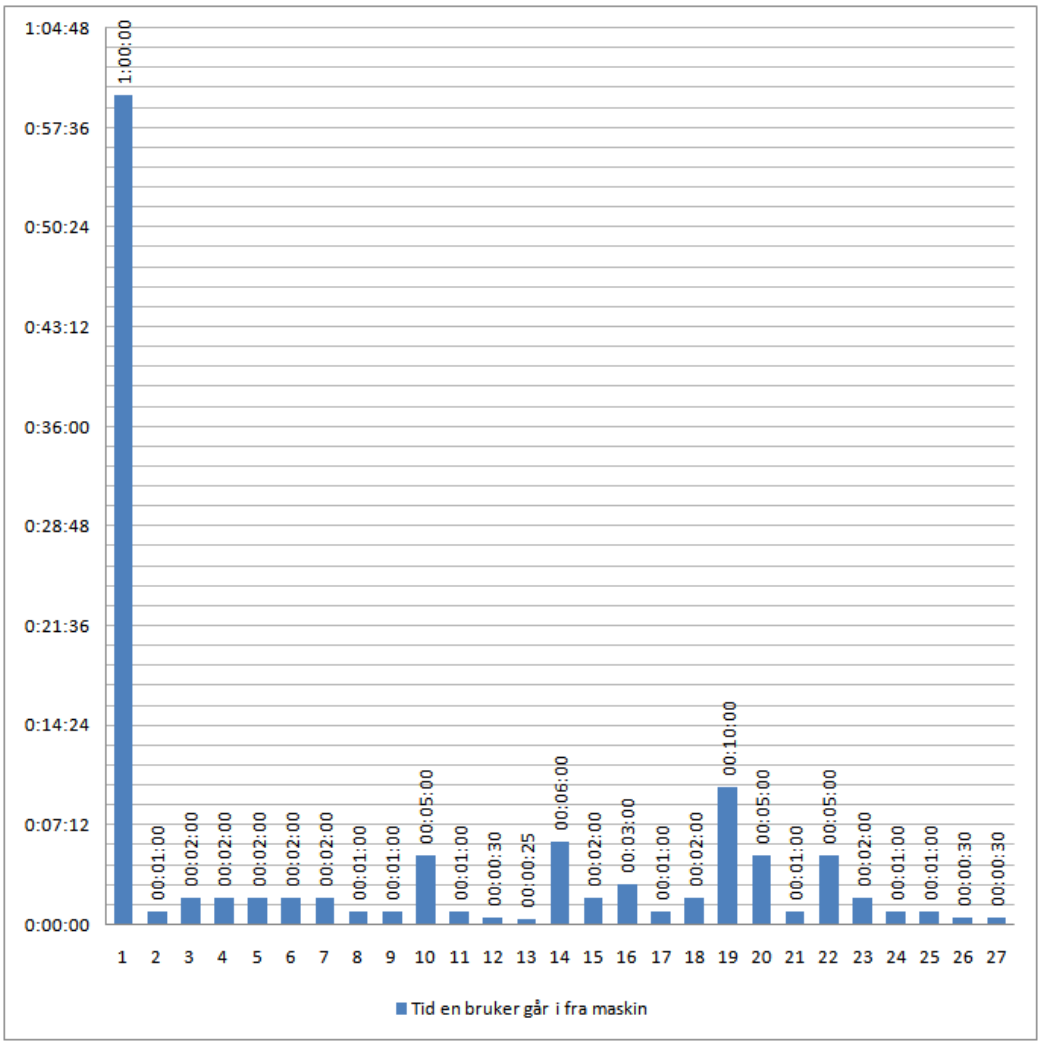
Totalt var det 7 av de 100 innloggingene som var usuksessfulle, altså 7 % totalt. Antallet regnes ut fra alle innlogginger på datamaskin, rørpost og telefon. Men for rørpost var alle innlogginger suksessfulle.

For de usuksessfulle innloggingene som ble registrert var det følgende systemer hvor bruker ikke fikk logget seg inn (med antall utifra de 7 usuksessfulle innlogginger) :

- Windows (2 tilfeller)
- DocuLive eller andre undersystemer inne i Windows (4 tilfeller)
  - DocuLive (2 tilfelle)
  - Ajourhold (1 tilfelle)
  - Min Arbeidsplan (1 tilfelle)
- IP telefon (1 tilfelle)

De usuksessulle innloggingene hadde forskjellige årsaker. Tallene er utifra de samme 7 usuksessfulle innlogginger som ovenfor bare nå kategorisert i årsaker. Årsakene er listet som følger:

- Maskin låst av annen bruker (1 tilfelle)
- Kort ikke aktivert enda (1 tilfelle)
- Ukjent innloggingsfeil for DocuLive (1 tilfelle)
- Bruker prøvde å loggge inn på nytt likevel programmet var åpent i bakgrunnen (1 tilfelle)



Figur 6.2: Tid brukere går ifra datamaskinen under en innlogging

- Feil passord (2 tilfeller)
- Ukjent innloggingsfeil for IP telefon (1 tilfelle)

En kommentar til årsaken feil passord: Hvis bruker tastet feil passord og ikke kom inn på første forsøk, men kom inn på andre forsøk ble det ikke regnet med som en usuksessfull innlogging og dermed ikke inkludert i denne statistikken.

Det kan også være andre grunner for usuksessfulle innlogginger. Denne informasjonen var kommentarer fra sykepleiere, hjelpepleiere eller leger som kom frem under intervjuer eller under observasjonene og var ikke egnet eller ment som et statistisk grunnlag. Dette vil heller bli oppsummert i delkapitlet for kvalitative data.

Avbrutte innlogginger

Avbrutte innlogginger inkluderer de tilfeller hvor brukeren ble avbrutt etter at selve innloggingssekvensen og autoriseringen var fullført. En vanlig grunn til dette var blant annet at brukeren måtte gå å gjøre noe annet. Dette skjedde ved totalt 8 av 100 innlogginger, altså 8 % totalt.

Avbrutte innloggingssekvenser inkluderer de tilfeller hvor brukeren måtte dro ut kortet og avbrøt innloggingen for å gå fra maskinen. Dette skjedde ofte i sammenheng med at enten en pasient eller en annen sykepleier kalte på den innloggende brukeren.

6.2.2 Kvalitative resultater fra observasjonene

Observasjonene hadde også en kvalitativ del. Denne ble samlet inn fra spesielle hendelser på avdelingen som var relatert med systemet eller brukerne, bruksvaner til de ansatte på avdelingen eller hvordan systemet fungerer i forhold til brukere og kontekst. Disse dataene ble notert ned under observasjonene og i sammenheng med samtaler med sykepleiere, hjelpepleiere og leger på avdelingen.

Lang innloggingstid

Innlogging på datamaskiner skjer ved at brukeren logger seg på først Windows med kort og pin, og i tillegg er det en innlogging med brukernavn og passord for undersystemene. Noe som ble fort lagt merke til under observasjonene var at tiden det tok å logge seg på systemet var gjerne svært lang, på både Windows og undersystemene. Som sett fra de kvantitative observasjonene var det i gjennomsnitt 1 minutt og 11 sekund. Noen av brukerne sa

at ventetiden oppleves ofte som lengre enn det også, siden de satt og så på skjermen og ventet.

I noen tilfeller måtte en i tillegg til å vente på sin egen innlogging vente på andre sin utlogging. I ett tilfelle ventet en lege i 50 sekunder på at forrige brukers profil skulle lagres og lukkes, før han kunne logge inn selv. I dette tilfellet brukte han også i tillegg 1 minutt og 4 sekunder på å logge inn på Windows, så 1 minutt og 17 sekunder på å logge inn på DocuLive. Det er en total innloggingstid på 3 minutter og 11 sekunder. Han skulle da bare inn å sjekke en opplysning på journalen og var inne i 50 sekunder før han logget ut igjen.

I noen tilfeller når det er lang innloggingstid på DocuLive blir brukeren utålmodig og trykker på DocuLive ikonet en gang til. Dette vil da i mange tilfeller hemme systemet enda mer og vil i mange tilfeller føre til at DocuLive aldri blir lastet så man kan logge seg inn. Brukeren må da logge ut og inn av Windows igjen for så å prøve igjen. I noen tilfeller tar de i bruk en annen datamaskin.

Akuttsituasjoner og trege datasystem

I de fleste situasjoner kan en bruker til nød tålerere trege datasystem og lang innlogging. Men i noen situasjoner står det om liv. Det er spesielt i akuttsituasjoner når sykehusansatte har behov for å bruke datamaskinene. Under observasjonene ble en slik situasjon registert. Det var ett spesielt tilfelle da en lege kom styrtende ut fra et pasientrom fordi det hadde oppstått komplikasjoner hos en pasient, og legen måtte kjapt få bestilt en CT og laget en henvisning på datamaskinen. I en situasjon har de ikke tid til å vente på en treg innlogging. Men han hadde flaks denne gangen fordi innloggingen Windows tok bare 30 sekunder, og han kom rett inn på DocuLive fra sin forrige sesjon.

Går ifra maskinen

På grunn av lang innloggingstid hadde mange hadde som vane å først logge på Windows med kort og kode først, for så å gå ifra maskinen med kortet i mens de ventet på at Windows skulle lastes. I mellomtiden kunne de gjøre noe annet. Når de da kom tilbake etter et par minutter kunne de da logge på undersystemene, for eksempel DocuLive. Men dette tok også et minutt til, så da måtte vente lenger. De kompenserte med dette med å gjøre flere oppgaver når de først var innlogget.

Når en bruker gikk ifra maskinen mens han eller hun ventet på at maskinen skulle logge seg på, hendte det seg også at når brukeren hadde vært borte

fra maskinen hadde hun startet på en annen oppgave der hun trengte kortet. Det kunne for eksempel være at hun eller han gikk inn på et pasientrom for å snakke med pasienten mens hun ventet på innloggingen, og da hadde hun funnet ut at pasienten trengte noe fra lageret, da trengte hun kort, og måtte da gå tilbake til datamaskinen for å hente dette. I slike tilfeller ble kortet ofte dratt rett ut uten å logge ut. Et tilfelle fra loggen er som følger: "Måtte gå ifra maskinen fordi en pasient spurte om han skulle gjøre noe mer i dag, så ho måtte gå å spørre. Ble borte i ca. 3 minutt. Gikk i fra maskinen totalt 4 ganger; 1 minutt andre gang, 2 minutt tredje gang, 10 minutt fjerde gang. Tredje gang var det for å gå å snakke med pasient, fjerde gang hadde ho gjort seg ferdig, tok med seg papira, men lot DocuLive stå åpent. Etter det kom ho tilbake fordi ho trengte kortet til medisinrommet, så ho måtte skrive ferdig i en fei og dra ut kortet."

Andre grunner til at en går fra maskinen er viss en skal skrive ut etiketter til prøver. Da skrives de ut fra datamaskinen, men man må gå til en skriver for å hente utskriften. Det er ikke skriver ved datamaskinene i fellesarealet hvor de ofte sitter, så da må de gå ifra maskinen og inn på kontoret eller pasientrommet. De vil selvsagt ikke logge ut i mellomtiden fordi det tar så lang tid å logge inn igjen, så da lar de maskinen heller stå åpen.

Ofte kan en bruker gå ifra maskinen opp til flere ganger per innlogging. I noen tilfeller har det blitt observert at en bruker har gått i fra hele både 3, 4 og 5 ganger. I tilfellet med 5 ganger var det en lege som var inne og sjekker på EPJ. Fra loggen: "Han har også med seg papirjournal og skjema som han skriver i mens han leser. Han går i fra maskinen og papir-journalen for å snakke med pasienten som sitter 10m borte i gangen. Går tilbake til maskinen igjen. Sitter i 5 minutt, går så inn på undersøkelserommet uten å logge ut, for å hente utskrift. Kommer tilbake for å legge den i journalen. Går ifra en gang til uten å logge av for å snakke med pasienten og gi han en sykemelding pluss resept. Går så tilbake til maskin en liten tur for å sjekke noe før han så går tilbake til pasienten. Går så tilbake til maskinen igjen. Pasienten kommer også bort til legen ved maskinen for å spørre om noe. Legen sitter og bruker diverse systemer blant annet kilden for å finne et nummer som han trenger for henvisningen. Går ifra en gang til til undersøkelsesrommet for å hente utskrift. Går så til pasienten igjen med utskrift så tilbake til maskinen."

Ulike årsaker til usuksessfulle innlogginger

Det opplevdes til tider at brukere ikke fikk logget seg på systemet. En oppfatning fra brukernes sin side var at dette var noe som skjedde relativt ofte. Dette stemte også i samsvar med observasjonene. I de tilfeller brukerne ikke hadde en suksessfull innlogging på grunn av feil passord, var det som regel en

av to grunner til at passordet var feil. Dette kom frem under samtaler med sykepleiere og hjelpepleiere på avdelingen. De to grunnene var som følger:

1. De hadde glemt passordet. Årsaken til dette var det kunne skyldes en av de følgende tre grunner:
   (a) Fordi de hadde vært borte på permisjon en stund og dermed ikke brukt systemet på flere uker eller måneder.
   (b) Passordet er til et system som ble sjelden brukt og som hadde et forskjellig passord fra andre systemer.
   (c) Fordi de hadde så mange passord å huske på for de forskjellige systemene at de blandet de sammen.
2. Passordet var gått ut på dato. På grunn av sikkerhetsårsaker går passordet ut på dato og man må skifte det etter en viss tid. De ulike systemene har ulik tidsperiode for hvor lenge et passord varer, derfor skifter man ikke passord på alle systemene samtidig, tidsperiodene for de ulike passordene kan være vanskelig å holde oversikt over.

6.3 Resultater fra intervjuer

Denne delen vil oppsummere resultater fra intervjuene. Intervjuene var i hovedsak kvalitative, derfor vil de kvalitative resultatene bli presentert først. I tillegg vil også noen kvantitative resultater bli presentert.

6.3.1 Kvalitative intervjuresultater

Denne første delen av resultatene vil starte med en oversikt over ulike systemer som blir brukt. I tillegg vil fordeler og ulemper hos det nåværende systemet som intervjuobjektene fortalte om bli presentert.

Oversikt over de brukte systemer

Her gis først en oversikt over de mest brukte systemene og med informasjon om hva de brukes til, hvem som bruker de og om systemet krever innlogging. Denne oversikten vil kort introdusere hvert system slik at man har noe å referere til når de blir nevnt i videre resultater og i analysen. Informasjonen i denne oversikten ble samlet inn fra intervjuene med de ansatte.

Pasientoversikten. Denne brukes mest av sykepleiere. Sykepleiere bruker det til å skrive inn og ut pasienter. De bruker det også til skrive ut

pasientliste med blant annet diagnose og utredning til de som kommer på neste vakt. Legene bruker det også til å holde oversikt. Pasientoversikten krever passord for innlogging.

DocuLive. DocuLive er det systemet som blir mest brukt av alle. Dette er hovedverktøyet for hjelpepleierene og sykepleierene. De bruker det primært til å skrive pleieplan og dokumentasjon om de pasienter de tar imot, der Det har blitt etterhvert et stort system med mange moduler, inkludert også RoS ("Remiss och Svar") der man kan få svar fra røntgen og andre labundersøkelser. Dette krever innlogging med brukernavn og passord.

PAS PAS er et system for pasientadministrasjon. Dette blir mest brukt av sykepleiere. Det brukes blant annet til å skrive inn og ut pasienter. Det blir også brukt til å skrive ut etiketter for prøver, finne informasjon om pasient som for eksempel telefonnummer for pårørende, registrere pasienter med kode i forhold til om de venter på rehabilitering eller om de er ferdig behandlet. Avdelingssykepleier bruker det til å skrive ut lister av og til, det er lister som pasientoversikt, venteliste, overflytting og utskrivning. Noen leger bruker det også en del. Noen få hjelpepleiere har også sagt at de bruker dette, for eksempel til å bestille urinprøver.

Kundrad Web. Dette programmet er det igjen sykepleierne som bruker mest. Dette blir mest brukt til å sjekke programmet for undersøkelser for neste dag, altså sjekke hvilke undersøkelser pasienter skal til (for eksempel røntgen eller MR (magnetresonanstomografi). Da ser de etter om leger har lagt inn henvisning til bildeundersøkelser, og man også se om røntgenavdelingen har satt opp time for pasientene. Det blir også brukt til å sjekke svar fra undersøkelser. Her må en logge inn. Kundrad Web er linket opp mot PACS/RIS (digital røntgen), som igjen er

PACS/RIS. PACS/RIS er digitalt røntgensystem som blir i hovedsak brukt av leger. Her kan de se på bilder fra røntgen, MR eller CT ("Computed Tomography"). Både PACS og RIS i tillegg til Kundrad Web er systemer levert av SECTRA[1]

Internett. Internett blir også brukt. Dette er noe alle de ulike ansatte bruker, det blir ofte brukt til finne informasjon som telefonnummer på for eksempel www.gulesider.no.

[1]SECTRA er et svensk selskap som leverer medisinske systemer og sikre kommunikasjonssystemer og som kjører på IDS5 webserver (også levert av SECTRA). Deres nettside er http://www.sectra.se/

Kilden. Det internettbaserte systemet Kilden blir også brukt av alle ansatte. Dette er "startsiden" på nettleseren, denne kommer opp ved oppstart av maskinen. Her finner en linker til tjenester og informasjon for helsetjenesten. Blant annet EQS og NELL, Legemiddelhåndboken, Felleskatalogen og Håndbok for labber. I EQS kan man gå inn og finne prosedyrer for hvordan ulike arbeidsoppgaver på sykehuset skal gjøres. Kilden krever ikke ekstra innlogging, men visse undersystemer inne i kilden gjør det, enten med personlig eller felles brukernavn/passord.

Min Arbeidsplan. Min arbeidsplan er et system der ansatte kan blant annet få oversikt over lønn, timer og vakter. Her må en logge inn, men dette er basert, og det finnes et valg for å lagre passordet til neste gang slik at en slipper å skrive inn passord hver gang. Dette systemet er også linket opp mot andre web-baserte tjenester med samme innlogging, og hvis man har lagret passordet sitt så vil man også få opp tilpasset informasjon til neste gang. Men dette er en funksjonalitet som har tatt i bruk, de fleste vet ikke om det, bare noen få unge entusiastiske erfarne databrukere vet om dette (faktisk var det bare en sykepleier jeg snakket med som viste om dette).

Outlook. Dette programmet trenger liten introduksjon. Outlook programmet fra Microsoft er det alle på sykehuset bruker som personlig e-post program. Her er innloggingsinformasjon lagret og man trenger ikke å skrive inn passord for hver gang man åpner programmet (Man må da i tillegg være påpasselig til at uvedkommende ikke får tilgang til en åpen og forlatt datamaskin). De har fått beskjed om at de må sjekke e-post i Outlook minst en gang for dag.

Op-plan. Dette blir også i hovedsak brukt av leger. Her får en oversikt over poliklinikkens ledige timer.

Ajourhold/Plansystem Dette er et system for å holde oversikt over turnus til de ansatte. Dette krever passord for innlogging. Det blir i hovedsak brukt av avdelingssykepleier og postsekretæren.

Nutshell (Matbestilling)] Matbestilling er det nå hjelpepleierne som har fått ansvar for. Dette bruker de et program som heter Nutschell. Matbestilling er noe som blir gjort en gang i uka så dette programmet er ikke så ofte brukt. Dette programmet krever enda et passord.

Transportbestilling Det finnes også et eget system for å bestille drosje, ambulanse, drosje og annen transport. Dette er det postsekretæren som

bruker mest.

Portørkom Det finnes også et eget system for å bestille portører. Dette er det postsekretæren som bruker mest.

Telefon På avdelingen finnes det trådløse IP-telefoner. De ansatte logger på hver sin om morgenen slik at de kan bli oppringt på fra de rom de har ansvar for. Disse er avbildet i figur 2.1(b).

Andre steder som krever autentisering

Det er ikke bare til datasystemet de ansatte på sykehuset trenger å autentisere seg. Under intervjuene ble de spurt hvilke andre steder de brukte å gå hvor de måtte autentisere seg. Her er en liste som følger med steder som krever autentisering. De fleste av disse stedene krever kort til å få adgang, noen også pin kode i tillegg. Noen steder krever autentisering kun på kveldstid.

- Inngangsdør bygget
- Personalinngang - Krever kort. (inngang på kveldstid)
- Inn mot kantine/ned til trappen - Krever kort.
- Kjeller - Krever kort+kode. I tillegg også fra kjelleren til neste kjeller for å hente matralle.
- Garderobe - Krever kort+kode. Kort også fra garderobe og opp.
- Tøyskap - Krever kort for å hente ut tøy.
- Medisinrom - Krever kort+kode. Hvis en er gruppeleder eller ansvar for medisinering er det ut og inn veldig mye.
- Avfallsrom - Krever kort.
- Møterom - Krever kun kort.
- Kontor - Krever kort.
- Skittentøyrom - Krever kort.
- Sengeheis - Blant annet heis til kjelleren. Eller for å få prioritet på heis, spesielt hvis en skal til undersøkelser.
- Rørpost - Må ha kode for å ta ut patronen av skapet.

- Sekretær - Krever kort. Hente journal
- Lager - Krever kort. Hente for eksempel stativ eller rullator
- Kontorfløyen - Krever kort.
- Rom med telefon - Krever kort i leser.
- Soverom nattevakt - Krever kort.
- Kundeservice - Krever kort.
- Andre avdelinger - Når en for eksempel går til Kvinne-Barn avdelingen eller når en går med pasienter til andre avdelinger.
- Soner - Må bruke kortet på soner med forskjellige farger. For eksempel grønne soner.
- Labsenteret - Krever kort+kode på kveldstid. For å gå med prøver, for eksempel for å levere spinalvæske.
- Klinisk - Krever kort på kveldstid. Levere prøver.
- Nevro intensiv - Krever kort.
- Avdelingen - Krever kort+kode for å komme seg inn om morgenen.
- På diverse andre dører - Kort uten kode.

Før sykepleierne og hjelpepleierne starter om morgenen må de bruke kortet på disse stedene:

1. Inngangsdør Bygget - Krever kort+kode.
2. Inn mot kantine/ned til trappa - Krever kort.
3. Ned i kjeller - Krever kort+kode.
4. Garderobe - Krever kort+kode.
5. Hente tøy - Krever kort.

Mangelfull dokumentasjon og lang innlogging

Mange sykepleiere og hjelpepleiere sa at de ikke får nok tid til å skrive dokumentasjon. Dette var blant annet på grunn av at systemet tok så lang tid til å logge på, og de hadde ikke tid til å vente på at systemet skulle logge seg på. Dermed brukte de ofte å enten ha en maskin stående på, for eksempel på undersøkelsesrommet slik at gå å gjøre andre oppgaver mens de var innlogget, eller de ventet med all dokumentering til slutten av dagen. Det som var dilemmaet med å vente med all dokumentasjon til slutten av dagen var at da hadde de mye oppsamlet arbeid og det ble mye å skrive. I tillegg blir de ofte avbrutt av andre ansatte eller pasienter. Alle deltakerne sa også at de foretrakk å gjøre arbeid på en datamaskin stille og rolig sittende ned så de slipper forstyrrelser fra andre. De vil helst prioritere pasientene, og dermed blir dokumentasjon nedprioritert.

Alle deltakerne under intervjuet kunne bekrefte at de hadde opplevt at de ikke fikk gjort en oppgave på grunn av at påloggingen mislyktes eller tok for lang tid. Det var noe som skjedde ofte. De fleste svarte at dette var noe som skjedde daglig.

Flere deltakere på intervjuene rapporterte at de hadde opplevd at det var mangelfull dokumentasjon på EPJ, og at dette hadde en direkte kobling med lang innloggingstid. Ingen kunne si at mangelfull dokumentasjon hadde ført til alvorlige hendelser men at det førte til at det går utover effektiviteten i den forstand at ansatte må repetetivt spør andre ansatte om informasjon om pasienter som istedet for kunne ligge i systemet. De bruker også mye tid til å lete etter informasjon som for eksempel telefonnummer. Her er det ofte vanlig at en går inn på Gulesider på internett istedet for i systemet for å finne telefonnummer til for eksempel pårørende til pasienter. Dette er noe som egentlig skal fylles ut ved pasientinnkomst.

Informasjon tilgjengelig for andre

Dataskjermene ved avdelingen er plassert ved skranken i fellesområdet. Mange av de spurte svarte at det var et problem med at siden skjermene sto slik de gjør kan det skje at informasjon på en skjerm har blitt tilgjengelig for andre enn de som skal ha tilgang. Dette er en stor utfordring, men de er oppmerksomme på det og passer på hele tiden.

De kunne også fortelle at i noen situasjoner har det skjedd at en når bruker har dratt kortet rett ut av datamaskinen, og når en annen bruker så logget seg inn med sitt kort, så fikk de opp samme sesjon. Dette er ikke noe som skal skje, og det er alvorlig sikkerhetsfeil. I dette tilfellet er det tydelig at en feil i systemet er kilde til et sikkerhetshull.

Integrasjon i systemer og mange passord

På sykehuset er det nødvendig med mange ulike systemer fordi der ikke er ett system som har absolutt all funksjonalitet man trenger. Derfor skaper dette også vanskeligheter med at disse systemene ikke er integrerte med tanke på innlogging. En ansatt må derfor holde oversikt over mange ulike passord, brukernavn og pin koder.

En lege fortalte at når han ble ansatt fikk han en e-post der det sto fem forskjellige passord og

Autentisering for flere ved samme skjerm

Et spørsmål som ble stilt i intervjuet var om de hadde hatt bruk for at flere kunne logge seg inn på en maskin samtidig. De fleste så ikke poenget i dette. Men en lege mente det kunne være nyttig når en overlege skal signere på noe han (lege) har skrevet, for eksempel epikrisen[2]. Epikrisen skal signeres av overlegen for godkjenning. Hvis legen har diktert ferdig epikrisen, og den er klar til signering av overlegen, kunne det vært nyttig om overlegen da kunne signert

6.3.2 Kvantitative intervjuresultat

Intervjuene ble utført i hovedsak som kvalitative dybdeintervju med en intervjuguide, men en del av dataene er mulig å presentere i kvantitativ form. Det gjelder statistikk på hvor mange som oppgav at de bruker visse systemer, og hvor mange ganger de logger inn på hvert system.

De ulike systemene og bruken av de

De systemer og programmer som ble brukt av de spurte intervjudeltakerene er vist i tabell 6.1. Andre kolonnen viser også hvor stor andel av de spurte som oppgav at de brukte dette systemet. Det er ikke sikkert at disse tallene er generaliserbare for andre deler av sykehuset. Det er heller ikke sikkert at de er representative for denne avdelingen. Siden de ansatte bruker mange forskjellige systemer, i tillegg til av at noen av de har overlappende funksjonalitet, kan det være at noen systemer ble utelatt under intervjuet. Det kan derfor være tilfeller der noen intervjuobjekter ikke oppga at de brukte et system på grunn av at de ikke husket på alle systemene når de ble spurt om hvilke systemer de bruker. Men denne systene som er opplistet i tabell 6.1 gir en viss pekepinn på hvilke av programmene som er de mest brukte.

[2]En epikrise er rapporten som skrives etter at en pasient har fullført et opphold. Epikrisen skal da følge med pasienten.

System	Antall som oppgir at de bruker
DocuLive	20 / 20
ROS/Labsvar (i Doculive)	7 / 20
KundradWeb	14 / 20
PAS	14 / 20
Pasientoversikten	4 / 20
Internett (Gulesider, Finn.no)	6 / 20
Kilden	6 / 20
EQS	6 / 20
NELL	2 / 20
Felleskatalogen	2 / 20
Legemiddelhåndboken	1 / 20
Håndbok for labber	1 / 20
Min Arbeidsplan	3 / 20
Outlook	11 / 20
Op-plan	4 / 20
Nutshell (Matbestilling)	2 / 20
Ajourhold/Plansystem	2 / 20
Portørcom	2 / 20
Ambulansebestilling	1 / 20
Transportbestilling	1 / 20
Drosjebestilling	1 / 20
Word/PowerPoint/Excel	2 / 20
IDS5/PACS/RIS	4 / 20

Tabell 6.1: Systemer som blir brukt

Antall innlogginger per dag

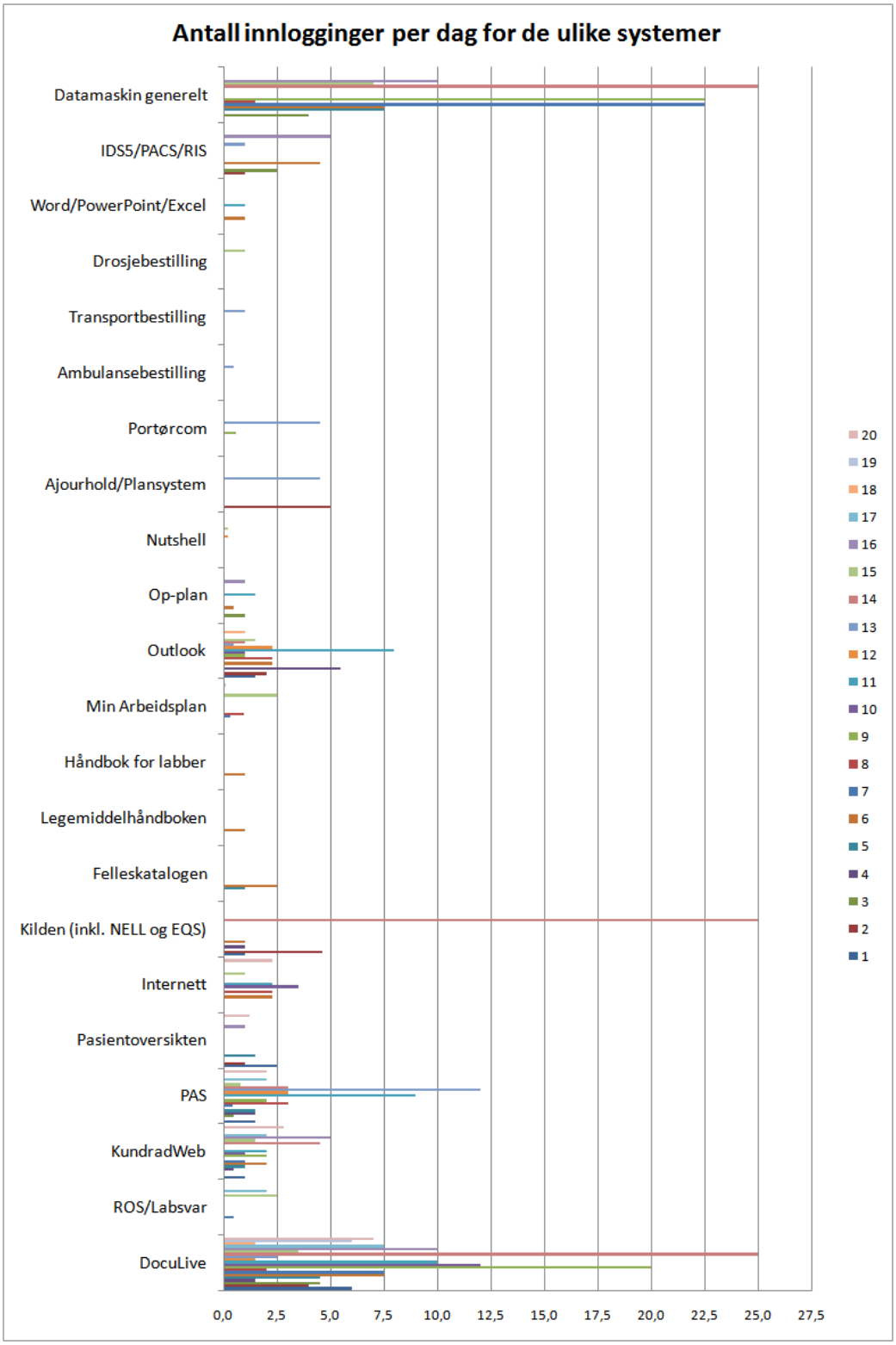
Under intervjuene ble det også spurt hvor mange ganger per dag de logget inn for hvert av de enkelte systemene. Et utregnet gjennomsnitt er vist i tabell 6.2. Gjennomsnittet er utregnet fra de personene som oppgav at de brukte systemet. Tabellen som er brukt som utregningsgrunnlag er lagt ved i tabell i Appendiks A, her er også gjennomsnittet tatt med. Fordeling av antall innlogginger er vist i stolpediagrammet i figur 6.3. Denne figuren viser resultatene fra alle systemene og fra alle intervjuobjektene. En stolpe i stolpediagrammet representerer antall ganger per dag en bruker har angitt at de logger på et system. Dette antallet gjelder for det systemet stolpen står ved. Fargekodene til høyre i diagrammet viser hvilke nummer deltaker som antallet innlogginger representerer. Man kan se at DocuLive og Kilden er de systemene der det er registrert høyest tall (25 innlogginger) i diagrammet. Men man ser også at Kilden har få stolper, dette tyder på at likevel Kilden er registrert med et høyt antall innlogginger for de som bruker det, er det få som har oppgitt at de bruker Kilden i forhold til for eksempel DocuLive. DocuLive er det systemet som har flest antall innlogginger. DocuLive er også det systemet som har flest brukere. Brukertallene kan man som nevnt se for antall stolper, men man kan også sjekke dette opp mot forrige tabell, tabell 6.1.

Antall innlogginger per dag for en bruker

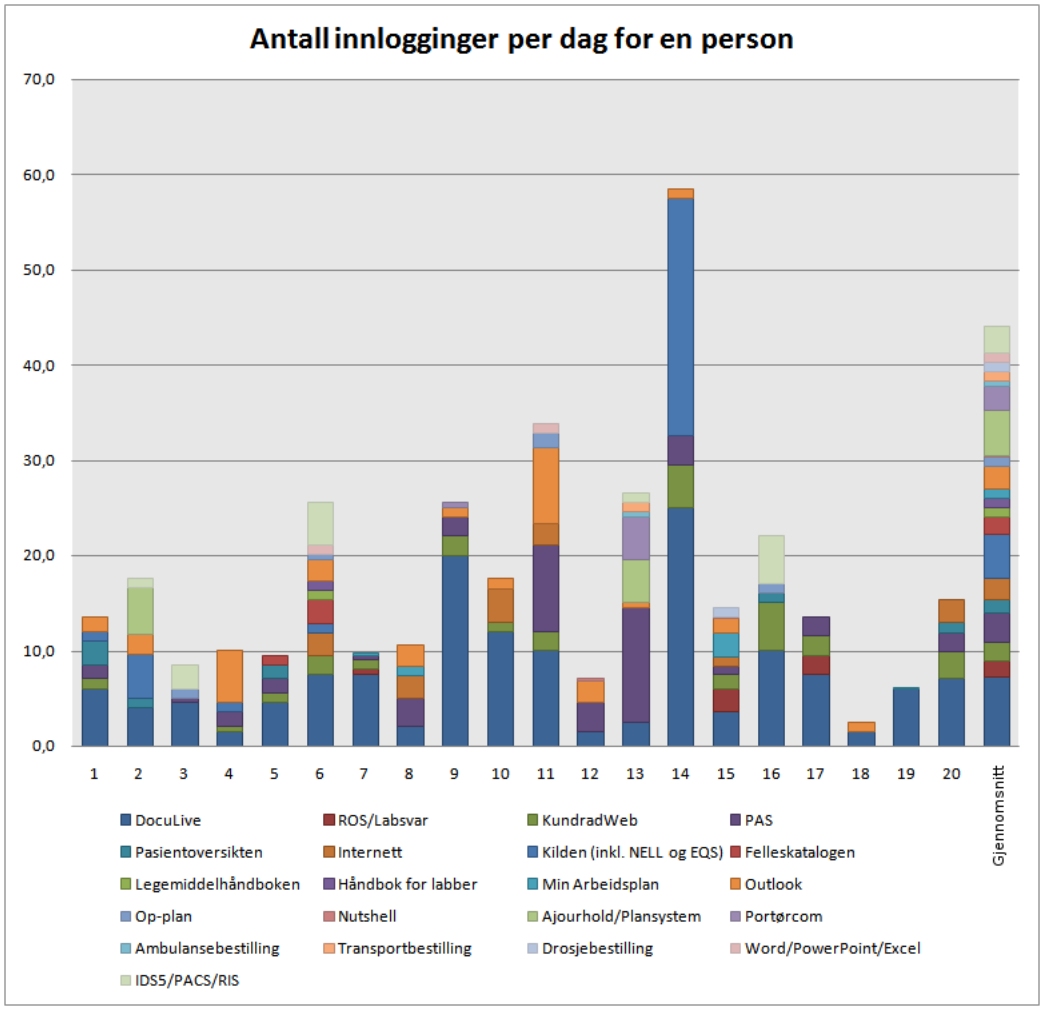
I søylediagrammet i figur 6.4 vises hvor mange innlogginger en bruker har per dag. Hver søyle representere summen av hvor mange innlogginger en bruker har per dag. Grunnlaget for disse talldataene finnes i tabellen som er lagt ved i Appendiks A.

System	Gjennomsnittlig antall innlogginger per dag
DocuLive	7,20
ROS/Labsvar (i Doculive)	1,5
PAS	2,35
Pasientoversikten	0,44
KundradWeb	1,45
Internett	2,27
Kilden (Inkl. EQS og NELL)	6,25
Felleskatalogen	1,75
Legemiddelhåndboken	1,00
Håndbok for labber	1,00
Min Arbeidsplan	0,97
Outlook	2,30
Op-plan	1,00
Nutshell (Matbestilling)	0,20
Ajourhold/Plansystem	4,75
Portørcom	2,55
Ambulansebestilling	0,50
Transportbestilling	1,00
Drosjebestilling	1,00
Word/PowerPoint/Excel	1,00
IDS5/PACS/RIS	2,80

Tabell 6.2: De mest brukte systemer



Figur 6.3: Antall innlogginger per dag for de ulike systemer



Figur 6.4: Antall innlogginger per dag for en bruker

Kapittel 7

Identifiserte problemer

I dette kapitlet vil de identifiserte problemer fra innsamlede data fra observasjoner og intervjuer spesifiseres. Dette er en oppsummering av de problemområder som er det mest hyppigste spesifisert etter hvilke type problem det medfører.

Problem 1: Lang innloggingstid

Lang innloggingstid er et problem som medfører unødig venting. Det hindrer dokumentasjon i den forstand at de ansatte ikke har tid til å vente på et tregt system og prioriterer derfor ikke å logge på datamaskiner. Det er spesielt lang innloggingstid i vaktskifte når det er mange som logger på, og rett før vaktskifte siden har ventet til da med å skrive dokumentasjon. Så problemet med lang innloggingstid har ringvirkninger: Man utelater å logge på for å dokumentere fordi systemet er treigt og innlogging tar lang tid, men man skaper mer treghet i systemet ved at man venter med å dokumentere til rett før vaktskifte.

Dette er et problem som har sin basis i oppbygningen av systemet, og at systemet er todelt: Man må først logge inn på operativsystemet Windows, og så logge inn på de underliggende systemene.

Problem 2: Går ifra maskin

Dette problemet et et av det største problemene når det gjelder sikkerheten for pasientdata. Det er et sikkerhetsproblem både for personvern av pasientdata i tillegg til at man setter systemet åpent for uvedkommmende som kan endre eller slette informasjon i systemet, eller utføre funksjoner som en ikke

er autorisert for (som i verste fall funksjoner som å skrive ut resepter til seg selv).

Dette problemet er i tillegg til et sikkerhetsproblem også et brukbarhetsproblem. Dette kan oppsummeres i følgende punkt delproblem:

- Delproblem P2.1: Går ifra maskin for å gjøre noe annet, uten å logge ut
  - Sikkerhetsproblem
    - andre kan se hva som er på skjermen
    - uautoriserte personer kan gå inn og lese informasjon som de ikke er autorisert for
    - uautoriserte personer kan gå inn å endre/legge til informasjon
  - Brukbarhetsproblem
    - dette er et brukbarhetsproblem i seg selv, de logger ikke ut fordi ikke vil bruke unødig tid på re-innlogging (også relatert til problem 1.
- Delproblem P2.2: Går ifra maskin for å gjøre noe annet, men logger ut
  - Brukbarhetsproblem
    - dette er et brukbarhetsproblem i seg selv, de logger ut fordi de må på grunn av sikkerhet, eller på grunn av at de trenger kortet annetsteds
    - treg pålogging når de skal inn igjen

Problem 3: Trenger kortet et annet sted

Dette er et problem som grunner i egenskapene til et smartkort. Dette er noe man må ha med seg for å bruke det, i tillegg til at innloggingsmekanismen på datamaskinene er laget slik at kortet må stå i for at man skal forbli innlogget.

Dette er også et underproblem av problem 2, men settes som et eget hovedproblem. Dette begrunnes med størrelsesordenen på problemet og at med en løsning på dette vil en eliminere andre hovedproblem.

Problem 4: Usuksessfull innlogging

Dette problemet er også et alvorlig problem. At man ikke kommer inn i systemet gjør at man ikke får tilgang til noe informasjon eller får gjøre noe

funksjoner som bare kan bli gjort inne i systemet. Grunner til dette følger. Disse er også sett på som underliggende relaterte problemer:

- Delproblem P4.1 - På grunn av feil med lokal maskin.
- Delproblem P4.2 - På grunn av feil i systemet (server)
- Delproblem P4.3 - På grunn av feil i overføring (ikke kontakt med server eller ressurs)
- Delproblem P4.4 - På grunn av treghet i overføring (kan være overbelastning i nettverk eller på server pga stor pågang)
- Delproblem P4.5 - På grunn av glemt brukernavn/passord/pin
- Delproblem P4.6 - På grunn av utgått passord/pin
- Delproblem P4.7 - På grunn av glemt/mistet kort

Problem 5: Mangel på integrasjon

Mangel på integrasjon mellom ulike systemer er på grunn av at systemene er ulike siden de er laget av forskjellige leverandører. Dette medfører at man har ulike standarder og mange ulike måter å logge seg på. Et delproblem her er at man får mange ulike brukernavn/passord/pinkoder.

Problem 6: Blir koblet av mens en er inne i et system

Et problem er at mens man er inne i et undersystem, for eksempel DocuLive, blir man koblet av dette systemet. Man må da ofte logge ut og inn igjen, eller logge inn på en annen maskin for at det skal løses. Grunnen til dette er ukjent.

Problem 7: Kommer inn i Windows, men kommer ikke inn i undersystemene

Et problem med et todelt system er at man må komme inn i begge for at man skal bli fullstendig innlogget. Et problem er at likevel man kommer inn i Windows er det ikke sikkert at man får gjort noe før man har suksessfullt fått logget inn i det ønskede undersystem som for eksempel DocuLive.

Kapittel 8

Krav til forbedringer

I dette kapitlet vil krav bli utarbeidet som et grunnlag for å løse problemene som ble identifisert. I utformingen av krav er det tatt utgangspunkt i at følgende punkter blir opprettholdt:

- Pasientene prioritet fortsetter å være i fokus
- Arbeidsoppgavene til de ansatte gis fokus
- Integritet for informasjonen i systemet
- Sikkerhet for pasient, ansatt og system
- De ovestående punkter skal kunne gjøres mer effektivt

For sikkerheten viktig at man tenker på hvilke situasjoner en ansatt egentlig trenger å bli autentisert. Det er ikke sikkert det trengst i alle situasjoner.

På et sykehus trengerer en ansatt å bli autentisert/gjenkjent for (1) adgangskontroll til informasjon i datasystemet (for eksempel elektroniske journaler, pasientregister, ansattregister) eller fysiske steder og utstyr (for eksempel kontor, pasientrom, dører, lager, bygninger), (2) dokumentere/registrere hvem som gjør hva og når, og (3) dokumentere/registrere hvem som har gått hvor og når. Dette kan oppsummeres i følgende punkter.

- Begrense tilgang (til digital/analog informasjon, til steder)
- Begrense tilgang til funksjoner /aktiviteter/gjøremål/operasjoner(både funksjoner i datasystemet(bestille røntgen) og ellers på sykehuset(ta blodprøve)
- Logge bruk (digitalt i datasystemet) (ellers i sykehuset også, viss man tenker på at ansatte og pasienter husker hvem som gjorde hva, men dette blir ikke logget digitalt)

Noe som kan settes som en kommentar for krav er at når man logger inn på sin tildelte konto på en datamaskin blir innstillinger og alle ressurser man har rettigheter til, koplet opp mot sin konto. Dette skjer hver gang man logger på, uansett hvilke ressurser man ville ha tilgang til. Men på et sykehus er det ikke bare snakk om å kontrollere tilgang, det er også strenge regler om at det skal holdes rede på hvem som har gjort hva. Derfor er det ofte unødvendig at systemet kjører en full innlogging med tildeling av ressurser og det hele, bare for å dokumentere hvem som gjorde hva. Så det kan være grunn til å tro at det muligens trengs en ny løsning for autentisering av brukere. Men først må en kartlegge hva som trengs og hvordan en ny løsning kan på en best mulig måte dekke dette behovet. Dette starter med å definere hva autentisering er både generelt og på et sykehus.

De følgende krav settes til et forbedret system:

8.1 Bedre oppfølging og dokumentering av pasientinformasjon

Dette kravet setter fokus på pasienten og gir krav om at det skal bli mer effektivt å dokumentere. Dette kravet tar fokus i at problemet med lang innloggingstid (Problem 1) gjør at dokumentering blir utelatt på grunn av dårlig tid.

8.2 Raskere og lettere tilgang til informasjon

Raskere og lettere tilgang til info setter fokus på at nye løsninger må eliminere problemet med lang innloggingstid og i tillegg vil eliminere at en trenger kortet et annet sted.

8.3 Bedre integrasjon mellom de ulike systemer

Dette vil gjøre at man vil beholde integrasjonen om informasjon mellom de ulike systemene og vil eliminere problemet med at brukere glemmer passordet.

8.4 Et mer stabilt system

Et mer stabilt system vil danne grunnlaget for at en kan hindre at problem med usuksessfulle innlogginger oppstår (problem 6), at man blir koblet av

mens man er inne i et system (problem 5), og at man kommer inn i Windows men ikke i undersystemene (problem 7).

Kapittel 9

Løsning på problem som kan tilfredsstille krav

Løsningene som presenteres her har som hovedmål å tilfredstille kravene som ble gitt, som igjen har som hovedmål å eliminere problemene og delproblemene. Denne løsning-krav-problem tilnærmingen fungerer da rekursivt ved at hvert nivå tar seg av elimineringen av sine delmål.

9.1 Bruk av fingeravtrykkslesere for identifisering av brukere

I følge evalueringen av autentifikatorer i introduksjonen er fingeravtrykk noe man alltid har med seg. Ved å innføre dette vil man dekke kravet om bedre oppfølging og dokumentering siden. Dette vil dekkes siden man ikke trenger å dra ut kortet hvis man trenger det et annet sted, og man trenger da heller ikke å logge seg på igjen. Dette vil igjen eliminere problemene med lang innlogging siden man ikke trenger å logge seg på så ofte. Dette vil også eliminere problemet med at bruker går ofte ifra maskinene. Eliminering av disse to tilsammmen vil føre til at brukerne kan dokumentere oftere, for eksempel innimellom andre oppgaver når man har tid.

9.2 Bruk av RFID

RFID [11] har den egenskapen at den kan autentisere en bruker på en viss avstand. Dette vil gjøre det mulig for en person å bli autentisert når den nærmer seg en datamaskin. Dette vil dekke kravet om raskere og lettere tilgang på informasjon. Denne teknologien kan da også brukes til å de-autentisere en

bruker hvis han går bort fra maskinen. RFID kan også brukes for lokalisering, man kan da få opp en liste på skjermen for de som er i nærheten og er identifisert, og brukere kan da raskt logge på en maskin.

9.3 Single sign on

Ved bruk av Single Sign-On [23] kan en bruker logge på mange systemer samtidig, dette dekker kravet om bedre integrasjon mellom de ulike systemene.

9.4 Samme sesjon for hver innlogging

Dette er ikke en teknologi som ble nevnt under introduksjonen, men er et tillegg som kan vurderes som en praktisk løsning som kan utføres på kort tid. Under dagens praksis ble det nevnt at hvis man drar kortet rett ut uten å logge ut med utloggingsknappen i Windows så skal man i prinsippet kommer direkte inn der man var under forrige innlogging. Men dette fungerer bare i noen få tilfeller, så derfor er det et fåtall som gjør det på denne måten. Noen leger og andre har som praksis å dra kortet rett ut, men de fleste gjør det ikke. Noen av sykepleierne og hjelpepleierne sier at de har fått beskjed om at ikke bør gjøre det på grunn av sikkerheten. Under observasjonene fant jeg ikke ut om en kommer direkte inn bare på den maskinen en var logget på forrige gang, eller om det fungerer kun med visse brukerkontoer. Hvis dette hadde fungert og det hadde blitt vanlig praksis for alle hadde mye med innloggingsproblematikken blitt løst er noe som det trengst mer detaljerte undersøkelser rundt. En mulig alternativ løsning for å få opp samme skjermbilde (eller sesjon) er også funksjonaliteten for som ligger innebygget i Windows XP som heter ”Raskt brukerbytte” (eng. ”Fast user-switching”). Her kan en bruker i stedet for trykke på ”Logg ut”, trykke på ”Bytt bruker”. Ved å da bytte til for eksempel en felles bruker, kan brukeren gå ifra maskinen uten at uvedkommende får adgang, og når denne brukeren kommer tilbake får han opp nøyaktig samme sesjon om han forlot. Når brukeren er ”utlogget” med ”Bytt bruker” tar det bare sekunder for å få tilbake samme sesjon etter at passordet er tastet inn. Andre brukere kan også i mellomtiden logge seg på maskinen uten at noen av programmene til forrige bruker blir berørt. Dette r noe som kan bli vurdert i fremtidige endringer av systemet.

Vurderingen som er gjort av nye løsninger og bruk av ny teknologi kan brukes som basis for design av et forbedret system

Kapittel 10

Diskusjon

Diskusjon vil omhandle en tolkning og utdypning av resultatene fra resultatene. Resultatene vil diskuteres opp mot teori og relevant forskning. Til slutt vil resultat og funn diskuteres opp mot en ideal løsning. I tillegg vil jeg diskutere de valg jeg har gjort gjennom oppgaven og muligheter for feilkilder ved resultatene og intervjuene.

10.1 Om observasjoner og intervju

Under observasjonene kunne det være perioder (på opptil noen timer) da det skjedde lite og det var lite bruk av datamaskiner, men tross i det måtte observasjonene fortsette som planlagt for å ikke miste data. Nytten av å observere over en tidsperiode på hele dager kom da virkelig frem, fordi i det hektiske sykehusmiljøet kunne det brått oppstå situasjoner som ga mye resultater også til den kvalitative delen av observasjonene. Observasjonene hadde på grunn av dette stor nytteverdi.

I etterkant av dette studiet ser man hva som kunne vært gjort annerledes. Ved analyse av resultatene ser man også at noen faktorer ved studiet kan føre til feilkilder i analysen.

Ved observasjonene kan det være at jeg ikke fikk sett alt som foregikk på alle maskiner på avdelingen siden jeg var alene som observatør. Jeg var heller ikke godt kjent med oppgavene de gjorde på avdelingen fra før, spesielt første tiden jeg var der, så det kan være tilfeller der jeg ikke har oppfattet den reelle meningen med visse oppgaver de gjorde.

Ved dybdeintervju kan det være en feilkilde at intervjuobjektet følte seg presset til å svare annerledes på noen spørsmål fordi de ikke var anonyme i forhold til intervjueren. Dette kan for eksempel være ved spørsmål som om de brukte å låne bort kortet sitt til andre. Her kan det være de ikke ville svare at

de lånte det bort siden de ikke har lov til det. Det var også noe som nettopp svarte det når jeg spurte om de hadde lånt bort kortet sitt; "Nei, det har vi ikke lov til". I noen tilfeller sa noen intervjuobjekter etter en stund, enten etter andre relaterte spørsmål eller når de hadde tenkt seg om; "Jo forresten, jeg har vel lånt det bort viss noen ikke hadde kortet sitt og de skulle inn en dør." Derfor kan det være at ikke alle svarte ærlig på slike spørsmål.

Jeg burde ha funnet ut i forkant hvilke systemer som finnes, slik at jeg da kunne spør om de brukte hvert enkelt system, istedet for å spør de hvilke systemer de bruker. For noen intervjuobjekter kan det være vanskelig å komme på systemene de bruker når de ikke har de foran seg på skjermen under intervjuet, og det er også mulig at noen utelatte noen fordi de kanskje trodde det ikke var viktig å nevne (som for eksempel Outlook).

10.2 Nye løsninger og kontekst

De nye løsningene krever ny teknologi som kan gjøre løsningene mulig. Slik teknologi er hele tiden under utvikling og det finnes eksempler på utprøvde teknikker [4]. I andre studier [[4] har slike studier vist seg å være lovende. Men før en eventuell implementasjon er det viktig at kontekst også tas i betraktning. Brukervennlighet gjelder alltid kun for den kontekst systemet skal bli brukt i. Mange av de nevnte studiene som sammenligner teknologi som er nevnt i introduksjonen og i kapitlet om relatert forskning bør vurderes sterkt i forhold til kontekst.

Kapittel 11

Konklusjon

Denne oppgaven har tatt for seg dagens praksis på sykehus. Observasjoner og intervjuer ble utført på Nevrologisk avdeling på St.Olavs sykehus. Disse har blitt oppsummert i form av resultater i både kvantitativ og kvalitativ form, og dannet basisen for oppsummering av problemer som har blitt kjent.

For å løse disse problemene har det blitt utarbeidet krav til løsninger. Til slutt har forslag til løsninger blitt utarbeidet på bakgrunn av kravene og problemene. Disse løsningene tar i bruk teknologi som er egnet til formålet. Hvor egnet disse teknologiene er til formålet er basert på tidligere forskning og andre sine evalueringer av disse.

Ved vurderinger av brukervennlighet og sikkerhet må disse to vurderes opp mot hverdandre. Som nevnt i introduksjonen har ofte har et sikkerhetsproblem grunnlag i brukervennlighet. Derfor må disse to settes opp mot hverandre og vurderes samtidig ved forandring av løsningenene til et system. Dette er særlig viktig med tanke på at innføring av nye sikkerhetsrutiner som ikke tar hensyn til at brukerne er en del av systemet, har en tendens til ikke blir brukervennlig, og dette igjen medfører at brukerne tar omveier i systemet for å lette hverdagen sin. Dette gir igjen sikkerhetsproblemer.

Bibliografi

[1] IButton. *What Is an iButton?*. Maxim Integrated Products. http://www.maxim-ic.com/products/ibutton/ibuttons/ Sist aksessert 5.juni 2008.

[2] International Standards Organisation, (1998), "ISO9241-11 Ergonomic requirements for office work with visual display terminals (VDTs) - Part 11: Guidance on usability", First Edition 1998-03-15, International Organisation for Standardisation Geneva.

[3] L.C.F. Araujo, Jr. Sucupira, L.H.R., M.G. Lizarraga, L.L. Ling, and J.B.T. Yabu-Uti. User authentication through typing biometrics features. *Signal Processing, IEEE Transactions on [see also Acoustics, Speech, and Signal Processing, IEEE Transactions on]*, 53(2):851–855, Feb. 2005.

[4] J. E. Bardram. The trouble with login: on usability and computer security in ubiquitous computing. *Personal Ubiquitous Comput.*, 9(6):357–367, 2005.

[5] Jakob E. Bardram, Rasmus E. Kjær, and Michael Ø. Pedersen. Context-aware user authentication - supporting proximity-based login in pervasive computing. In *UbiComp 2003: Ubiquitous Computing*, volume 2864/2003 of *Lecture Notes in Computer Science*, pages 107–123. Springer Berlin / Heidelberg, Berlin / Heidelberg, 2003.

[6] L. Bauer, L. Cranor, R. W. Reeder, M. K. Reiter, and K. Vaniea. Comparing access-control technologies: A study of keys and smartphones. Technical report, Carnegie Mellon University, 2007.

[7] Messaoud Benantar. *Access control systems: security, identity management and trust models*. Springer, 2006.

[8] Anita Campbell. U.S. School Children to be RFID-tagged. The RFID Weblog, 2005.

[9] Rogério de Paula, Xianghua Ding, Paul Dourish, Kari Nies, Ben Pillet, David Redmiles, Jie Ren, Jennifer Rode, and Roberto Silva Filho. Two experiences designing for effective security. In *SOUPS '05: Proceedings of the 2005 symposium on Usable privacy and security*, pages 25–34, New York, NY, USA, 2005. ACM.

[10] Alexander J. DeWitt and Jasna Kuljis. Aligning usability and security: a usability study of polaris. In *SOUPS '06: Proceedings of the second symposium on Usable privacy and security*, pages 1–7, New York, NY, USA, 2006. ACM.

[11] Klaus Finkenzeller. *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification, 2nd ed.* John Wiley and Sons, 2003.

[12] Anders Grimsmo. Medisinskfaglig analyse av behovet for enklere kommunikasjon i tilknytning til bruken av elektronisk pasientjournal. Report, Norsk senter for elektronisk pasientjournal, Trondheim, 03.09.2007 2007.

[13] Gunnar Hartvigsen. *Forskerhåndboken.* Høyskoleforlaget AS - Norwegian Academic Press, Kristiansand, 1998.

[14] ISO. ISO 13407: Human-centred Design Processes for Interactive Systems, 1999.

[15] Gary C. Kessler. An Overview of Cryptography. I: John P. Slone (red.), Handbook on Local Area Networks. Auerbach 1998. Online versjon tilgjengelig på http://www.garykessler.net/library/crypto.html, sist aksessert 5.juni 2008 , 1998.

[16] Alfred J. Menenez, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1996.

[17] Merriam-Webster's Collegiate Dictionary. Merriam-Webster's Collegiate Dictionary, from Encyclopaedia Britannica 2008 Ultimate Reference Suite DVD. Copyright © 1994-2007 Merriam-Webster, Inc., 2008.

[18] Lawrence O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12):2021–2040, 2003.

[19] Jennifer Preece, Yvonne Rogers, and Helen Sharp. *Interaction Design : Beyond Human Computer Interaction.* John Wiley and Sons, Inc., 2002.

[20] Wolfgang Rankl and Wolfgang Effing. *Smart Card Handbook, 2nd ed.* John Wiley and Sons, 2004.

[21] Eirik Rossen. Rfid-pass er sikkerhetsrisiko. digi.no, 27.des. 2004. http://www.digi.no/php/art.php?id=114515. sist aksessert 5.juni 2008, 2004.

[22] P. Rotter. A framework for assessing rfid system security and privacy risks. *Pervasive Computing, IEEE*, 7(2):70–77, April-June 2008.

[23] M. J. Sapp and T. L. Behrens. Single logon: Balancing security and healthcare productivity. *Journal of Healthcare Information Management*, 18(2):21–26, 2004.

[24] Andrew S. Tanenbaum. *Modern Operating Systems 2nd Ed.* Prentice-Hall, 2nd edition, 2001.

[25] Doroteo T. Toledano, Rubén Fernández Pozo, Álvaro Hernández Trapote, and Luis Hernández Gómez. Usability evaluation of multi-modal biometric verification systems. *Interacting with Computers*, 18(5):1101–1122, 2006. 1221459.

[26] VingCard. VingCard Elsafe a.s. http://www.vingcard.com/ . Sist aksessert 5.juni 2008, 2008.

Tillegg A

Tabeller fra intervjudata

Tabell A.1: Intervjudata. Antall innlogginger per dag for hver bruker

	Intervjudeltakernummer med antall innlogginger per dag																				
System	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Gj.sn.
DocuLive	6,0	4,0	4,5	1,5	4,5	7,5	7,5	2,0	20,0	12,0	10,0	1,5	2,5	25,0	3,5	10,0	7,5	1,5	6,0	7,0	7,20
ROS/Labsvar							0,5								2,5		2,0				1,67
KundradWeb	1,0			0,5	1,0	2,0	1,0		2,0	1,0	2,0			4,5	1,5	5,0	2,0			2,8	2,02
PAS	1,5		0,5	1,5	1,5		0,4	3,0	2,0		9,0	3,0	12,0	3,0	0,8		2,0			2,0	3,02
Pasientoversikten	2,5	1,0			1,5											1,0				1,2	1,44
Internett						2,3		2,3		3,5	2,3				1,0					2,3	2,27
Kilden (inkl. NELL og EQS)	1,0	4,6		1,0		1,0								25,0							4,63
Felleskatalogen					1,0	2,5															1,75
Legemiddelhåndboken						1,0															1,00
Håndbok for labber						1,0															1,00
Min Arbeidsplan							0,3	1,0							2,5				0,1		0,97
Outlook	1,5	2,0		5,5		2,3		2,3	1,0	1,0	8,0	2,3	0,5	1,0	1,5			1,0			2,30
Op-plan			1,0			0,5					1,5					1,0					1,00
Nutshell												0,2			0,2						0,20
Ajourhold/Plansystem		5,0											4,5								4,75
Portørcom									0,6				4,5								2,55
Ambulansebestilling													0,5								0,50
Transportbestilling													1,0								1,00
Drosjebestilling															1,0						1,00
Word/PowerPoint/Excel						1,0					1,0										1,00
IDS5/PACS/RIS		1,0	2,5			4,5							1,0			5,0					2,80
Datamaskin generelt			4,0		7,5	7,5	22,5	1,5	22,5					25,0	7,0	10,0					11,94