Multilevel Security: Systemer med gradert informasjonsflyt

av

Per Gøran Bergerud
Gyda Ellefsplass Olssen

Masteroppgave i
informasjons- og kommunikasjonsteknologi

Høgskolen i Agder
Fakultet for teknologi

Grimstad
mai 2005

Sammendrag

I forbindelse med utviklingen og innføringen av et Felles Integrert Forvaltningssystem (FIF), trenger Forsvaret en løsning for sikker gradert informasjonsflyt. Et begrep som omhandler denne problematikken er Multilevel Security, som har vært et viktig tema i forsvarssammenheng siden begynnelsen på syttitallet. Til tross for at Multilevel Security har vært et tema i snart førti år, foreligger det fortsatt ingen fullverdig løsning for bruk i forsvarssammenheng.

Med bakgrunn i dette har vi kartlagt situasjonen innen Multilevel Security, og redegjort for ulike teorier og strategier på området. Oppgaven er videre delt inn i tre delproblemer. Det første dreier seg om hvilke sikkerhetskrav som vedrører Multilevel Security, det andre tar for seg kartlegging av teorier, strategier og realiserte systemer innen Multilevel Security, og det siste dreier seg om konsekvenser ved en eventuell implementering av Multilevel Security i Forsvaret.

Selv om oppgaven primært er skrevet for Forsvaret, kan mange av funnene være av interesse for andre. Det kan for eksempel være private eller offentlige bedrifter som har behov for informasjonsflyt med sensitive opplysninger.

Resultatene fra det første delproblemet viser at Sikkerhetsloven og NATOs sikkerhetsbestemmelser setter grenser for, og stiller krav til, sammenkoblinger av systemer med forskjellige graderingsnivåer. Dette er trolig den største utfordringen med tanke på en eventuell innføring av Multilevel Security i Forsvaret. Videre må Multilevel Security-systemer tilfredsstille evaluerings- og sertifiseringskrav i Common Criteria. Dette er etter vår mening med på å dempe viljen til å utvikle og innføre nye Multilevel Security-systemer. Vi konkluderer med at gjeldende krav og evalueringskriterier må endres, for at Multilevel Security noensinne skal kunne innføres i Forsvaret.

I det andre delproblemet har vi har valgt ut seks modeller, en strategi og en metode. Disse representerer et historisk snitt fra den første Multilevel Security-modellen fra 1973, til en aktuell metodisk prosess fra slutten av nittitallet. Vi har sammenliknet modellene, strategien og metoden i et rammeverk, der vi har sett på hvilke egenskaper som vedrører modellene. Videre har vi presentert et utvalg av realiserte Multilevel Security-systemer. Mange av disse systemene er bygd på den klassiske Bell-LaPadula-modellen. Det finnes imidlertid få nye systemer, og vi etterlyser derfor en ny formell modell. Denne må tilpasses dagens teknologi og krav, og veilede utviklingen av fremtidige Multilevel Systemer.

I det tredje delproblemet har vi kommet frem til at Multilevel Security trolig vil forenkle og effektivisere arbeidsdagen til de ansatte. De ansatte vil sannsynligvis få mer tid til å utføre sine primærfunksjoner, i stedet for å bruke tid på å skifte mellom systemer. Samtidig vil en

innføring av et Multilevel Security-system sette høye krav til brukerne, siden et slikt system ikke innehar noen fysisk sperring mellom graderingsnivåene. En eventuell innføring av Multilevel Security i Forsvaret vil bli svært kostbart, med tanke på implementering og opplæring. Vi mener imidlertid en slik investering vil bli lønnsom over tid.

Forord

Denne oppgaven representerer avslutningen på et femårig mastergradsstudium i informasjons- og kommunikasjonsteknologi ved Høgskolen i Agder. Oppgavens arbeidstittel, Multilevel Security: Systemer med gradert informasjonsflyt, er gitt av Forsvarets Program Golf. Oppgaven er utført med veiledning fra hovedveileder, professor Per Egil Pedersen, og teknisk veileder, overingeniør Hans Petter Egeland. Arbeidet med oppgaven er hovedsakelig gjennomført på Høgskolen i Grimstad.

Vi vil først og fremst rette en stor takk til professor Per Egil Pedersen, for god hjelp og rettledning under hele prosjektperioden. Vi vil videre rette en takk til overingeniør Hans Petter Egeland, for en utmerket jobb som kontaktperson og teknisk veileder. Videre vil vi takke våre ressurspersoner i Program Golf, IBM og FLO/IKT.

Grimstad, mai 2005.

Per Gøran Bergerud og Gyda Ellefsplass Olssen

Innholdsfortegnelse

SAMMENDRAG ..... **I**

FORORD ..... **III**

INNHOLDSFORTEGNELSE ..... **IV**

FIGURLISTE ..... **VI**

TABELLISTE ..... **VI**

1 INNLEDNING **1**

1.1 BAKGRUNN OG PROBLEMOMRÅDE 1
1.2 PROBLEMSTILLING 1
1.2.1 Delproblemer *1*
1.3 PROBLEMAVGRENSNINGER OG FORUTSETNINGER 2
1.4 BEGREPSDEFINISJONER 2
1.5 MILITÆR SIKKERHETSSTRUKTUR 3

2 LITTERATURREVIEW **4**

2.1 GENERELLE KRAV TIL INFORMASJONSBEHANDLINGSSYSTEM 4
2.2 TILGANGSKONTROLL 4
2.2.1 Discretionary Access Control *4*
2.2.2 The Role-based Access Control Model *5*
2.2.3 Mandatory Access Control *7*
2.2.4 Sikkerhetsmekanismer *9*

3 MULTILEVEL SECURITY **13**

3.1 INTRODUKSJON 13
3.1.1 Bakgrunn *13*
3.1.2 Sikkerhetsnivåer *13*
3.1.3 Operasjonsmåter *15*
3.1.4 MLS-mekanismer *15*
3.2 SIKKERHETSUTFORDRINGER 16
3.2.1 Trojanske hester *16*
3.2.2 Skjulte kanaler *16*
3.2.3 Begrensninger i Multilevel Security -systemer *17*
3.2.4 Tillitsproblemet *17*

4 METODE **19**

4.1 GENERELT 19
4.2 METODISK TILNÆRMING 19
4.3 TILNÆRMING FOR HVERT DELPROBLEM 20
4.3.1 Delproblem 1 ..... *20*
4.3.2 Delproblem 2 ..... *22*
4.3.3 Delproblem 3 ..... *22*
4.4 KVALITATIVE UNDERSØKELSER 23
4.4.1 Kvalitativ undersøkelse 1 ..... *24*
4.4.2 Kvalitativ undersøkelse 2 ..... *26*

5 RESULTATER **28**

5.1 DELPROBLEM 1: GJELDENDE SIKKERHETSBESTEMMELSER 28
5.1.1 Bakgrunn 28
5.1.2 Metode 29
5.1.3 Sikkerhetskrav i gjeldende lovverk 29
5.1.4 Synspunkter vedrørende gjeldende sikkerhetskrav 33
5.1.5 Oppsummering 35
5.2 DELPROBLEM 2: KARTLEGGING AV MULTILEVEL SECURITY 36
5.2.1 En kort historisk oversikt 36
5.2.2 Hva skjedde etter 1990? 36
5.2.3 Metode 37
5.2.4 Bell-Lapadula-modellen 41
5.2.5 Revidert Bell-La Padula 43
5.2.6 Den Militære Meldingsmodellen 44
5.2.7 SNet-modellen 47
5.2.8 A Multilevel Security Policy Model for Networks 51
5.2.9 An Execution Model for Multilevel secure Workflows 53
5.2.10 MLS Workflow Management System 57
5.2.11 Domain Based Security 62
5.2.12 Multilevel Security i dag og i fremtiden 66
5.2.13 Oppsummering 73
5.3 DELPROBLEM 3: KONSEKVENSER VED INNFØRING AV MULTILEVEL SECURITY 76
5.3.1 Bakgrunn 76
5.3.2 Metode 76
5.3.3 Resultater 77
5.3.4 Oppsummering 81

6 DRØFTING 82

6.1 INNLEDNING 82
6.2 GJELDENDE KRAV 82
6.2.1 Sikkerhetskrav 82
6.3 EVALUERINGSKRITERIER 83
6.4 TEORIER OG STRATEGIER INNEN MULTILEVEL SECURITY 84
6.5 REALISERTE MULTILEVEL SECURITY -SYSTEMER OG SYSTEMER I FORSVARET I DAG 86
6.6 KONSEKVENSER VED INNFØRING AV MULTILEVEL SECURITY 87
6.7 VALIDITET 89
6.7.1 Kvalitativ undersøkelse 1 89
6.7.2 Delproblem 1 90
6.7.3 Delproblem 2 90
6.7.4 Delproblem 3 91

7 KONKLUSJON 94

7.1 FORSLAG TIL VIDERE FREMDRIFT 94

8 FORKORTELSER 97

9 LITTERATURLISTE 98

10 VEDLEGG 102

VEDLEGG A: INTERVJUGUIDE TIL KVALITATIV UNDERSØKELSE 1 102
VEDLEGG B: RESULTATER FRA KVALITATIV UNDERSØKELSE 1 102
VEDLEGG C: SPØRRESKJEMA TIL KVALITATIV UNDERSØKELSE 2 102
VEDLEGG D: SKJEMATISKE RESULTATER TIL KVALITATIV UNDERSØKELSE 2 102

Figurliste

FIGUR 1: RBAC (LAGET UT IFRA SAMARATI & VIMERCATI, 2001). 6
FIGUR 2: ROLLEHIERARKI. 6
FIGUR 3: EKSEMPEL PÅ EN NPD-RETTIGHETSGRAF (LAGET UT IFRA SAMARATI & VIMERCATI, 2001). 7
FIGUR 4: INFORMASJONSFLYT I BIBA-MODELLEN (LAGET UT IFRA SAMARATI & VIMERCATI, 2001). 8
FIGUR 5: EKSEMPEL PÅ THE CHINESE WALL (LAGET UT IFRA BREWER & NASH, 1989) 9
FIGUR 6: THE NRL PUMP. 11
FIGUR 7: HIERARKISKE SIKKERHETSNIVÅER. 14
FIGUR 8: METODISK TILNÆRMING. 20
FIGUR 9: ET EKSEMPEL PÅ TILGANGSKONTROLL I BLP-MODELLEN. 42
FIGUR 10: SNET ARKITEKTUR (LAGET UT IFRA GLASGOW & MACEWEN, 1987). 47
FIGUR 11: ET ABSTRAKT OPERATØRNETT (LAGET UT IFRA GLASGOW & MACEWEN, 1987) 49
FIGUR 12: ET RAFFINERT ABSTRAKT OPERATØRNETT (LAGET UT IFRA GLASGOW & MACEWEN, 1987) 50
FIGUR 13: EKSEMPEL: OPPGAVEBINDINGER I MLS-ARBEIDSFLYT (LAGET UT IFRA ATLURI ET AL., 1997). 56
FIGUR 14: KATEGORISERING AV HIGH-TO-LOW-BINDINGER (LAGET UT IFRA ATLURI ET AL., 1997). 56
FIGUR 15: EN MLS DISTRIBUERT ARKITEKTUR (KANG ET AL. , 1999). 59
FIGUR 16: INFORMASJONS-, FRIGIVELSE-, OG MOTTAKSPOLITIKKER (KANG ET AL., 1999). 60
FIGUR 17: EKSEMPEL PÅ EN METEOR-MODELL. 61
FIGUR 18: INFORMASJONSSIKRE KRAVMODELLER (LAGET UT IFRA ROBINSON, 2001) 62
FIGUR 19: EN ENKEL FIRMAMODELL. 63
FIGUR 20: MODELL SOM VISER MILJØENE. 64
FIGUR 21: TO INFRASTRUKTURØYER. 64
FIGUR 22: EKSEMPEL PÅ ET DOMENEBASERT NETTVERK. 65

Tabelliste

TABELL 1: TILGANGSKONTROLLPOLITIKKER MED TILHØRENDE MODELLER. 4
TABELL 2: EKSEMPEL PÅ TILGANGSKONTROLLMATRISE. 5
TABELL 3: OVERSIKT OVER DE MODELLENE, STRATEGIEN OG METODEN VI HAR VALGT. 39
TABELL 4: OVERSIKT OVER VALGTE MLS–SYSTEMER. 40
TABELL 5: SAMMENLIKNING AV MODELL EGENSKAPER. 73
TABELL 6: OPPSUMMERING AV MLS–SYSTEMENE. 75
TABELL 7: OVERSIKT OVER DE MODELLENE, STRATEGIEN OG METODEN VI HAR VALGT. 84
TABELL 8: OVERSIKT OVER VALGTE MLS-SYSTEMER. 86

1 Innledning

1.1 Bakgrunn og problemområde

For å kunne tilfredsstille de krav som stilles Forsvaret om styring og kontroll, samt betydelig reduksjon av kostnader til drift og forvaltning, er Forsvaret nå inne i en omstillingsfase der de søker å effektivisere prosesser på tvers av grenene gjennom felles bruk av ressurser. Tidligere brukte Forsvaret i overkant av 170 ulike systemer for å forvalte ressurser og materiell (Program Golf).

Forsvaret etablerte Program Golf våren 2000. Programmet ble tildelt ansvaret for å lede arbeidet med å utvikle og innføre et Felles Integrert Forvaltningssystem (FIF) for hele Forsvaret. Program Golf gjennomføres som flere prosjekter som til sammen skal gi Forsvaret et helhetlig system for forvaltning innen personell-, økonomi- og materiellfunksjoner.

Det norske forsvaret har, i likhet med mange andre forsvarsnasjoner, et håp om å innføre Multilevel Security (MLS) i fremtiden. MLS er som navnet sier et konsept for en flernivås sikkerhetsløsning. Utviklingen startet på syttitallet, da det amerikanske forsvarsdepartementet opprettet noen sikkerhetsprosjekter som skulle formalisere sikker informasjonsflyt i nettverkene. MLS sikrer at data kan sendes over en enkel infrastruktur, samtidig som det oppnås høyeste sikkerhet. Det betyr at bare autoriserte brukere får tilgang til informasjonen. Det har med årene kommet flere modeller, metoder og strategier for hvordan en skal oppnå MLS. Blant flere lands forsvar, er det kanskje USA som har kommet lengst i utviklingen av gode MLS-løsninger.

1.2 Problemstilling

Forsvaret er i ferd med å utvikle og innføre et FIF for hele organisasjonen. Samtidig skal Forsvaret utvikles i retning av et Nettverksbasert Forsvar (NbF) der systemunderstøttelsen i størst mulig grad er lik i alle situasjoner. I den forbindelse mangler Forsvaret en løsning for sikker gradert informasjonsflyt. MLS er et konsept som kan løse dette. På bakgrunn av dette formulerte vi følgende problemstilling for oppgaven:

Vi skal kartlegge situasjonen innenfor Multilevel Security og redegjøre for teorier og strategier på området. På grunnlag av dette skal vi vurdere ulike løsninger for Forsvaret.

1.2.1 Delproblemer

Basert på problemstillingen over har vi laget tre mer konkrete delproblemer for oppgaven. I første omgang måtte vi få en oversikt over hvilke krav Forsvaret har i forhold til informasjonssikkerhet vedrørende MLS. Informasjonssikkerheten i alle systemer må ivareta tjenstlige behov og beskytte sensitiv informasjon. Det første delproblemet formulerte vi derfor som følger:

1. *Vi skal systematisere Forsvarets krav til systemer som sammenkobler informasjon med ulik sikkerhetsgradering.*

Videre måtte vi kartlegge situasjonen innenfor MLS og redegjøre for teorier og strategier på området. Det andre delproblemet formulerte vi følgelig som:

2. *Vi skal redegjøre for teorier og strategier innen MLS, samt presentere realiserte MLS-systemer.*

For å kunne vurdere hvilke MLS-løsninger som er best egnet for Forsvaret, ble vi nødt til å redegjøre for konsekvensene for en eventuell innføring av et slikt konsept. Det tredje delproblemet definerte vi som følger:

3. *Vi skal utrede konsekvensene av innføringen av et system som sammenkobler informasjon med ulik sikkerhetsgradering.*

1.3 Problemavgrensninger og forutsetninger

Når det gjelder utredning av konsekvenser for en eventuell innføring av MLS i Forsvaret, har vi ikke tatt hensyn til kostnader, tidsperspektiv eller opplæring. Vi har konsentrert oss om konsekvenser i forhold til sikkerhet og bruksnytte.

Forsvaret har valgt SAP som Enteprice Resource Planning (ERP) -system, siden dette er det eneste ERP-system, som har en egen modul for forsvarsrelaterte tjenester. I vår oppgave har vi ikke sett på hvordan MLS kan integreres i SAP.

I forbindelse med systematiseringen av Forsvarets krav til informasjonssikkerhet, har vi tatt for oss konfidensialitet, integritet og tilgjengelighet.

1.4 Begrepsdefinisjoner

Tilgang til informasjon innad i Forsvaret er basert på gradering av informasjon, brukerklarering og autorisasjon. Sikkerhetsloven og sikkerhetsbestemmelser i NATO setter grenser og gir krav til sammenkoblinger av systemer med forskjellige graderingsnivåer. Forsvaret er som sagt i ferd med å utvikle og innføre FIF for hele organisasjonen. Dette er et system som skal implementeres innen områdene økonomi, logistikk, personell og ledelse & styring, og skal medvirke til effektivisering av prosesser på tvers av forsvarsgrenene gjennom felles bruk av ressurser.

I problemstillingen har vi brukt uttrykket sikker gradert informasjonsflyt. Med sikker mener vi at det ikke er mulig for uvedkommende å få tilgang til informasjonen, det vil si at det bare er adressaten(e) som får tilgang til den aktuelle informasjonen. Gradert informasjonsflyt betyr utveksling av informasjon uten at dette styres manuelt.

Vi har brukt ordet informasjonssikkerhet i formuleringen av det første delproblemet. Informasjonsflyt deles ofte inn i fire hovedområder: autentisering, konfidensialitet, integritet og tilgjengelighet. Disse fire områdene henger nøye sammen når egenskaper innen sikkerhet skal beskrives. Det er vanskelig å oppnå sikkerhet uten pålitelighet. Et sikkert system må også til en viss grad være robust, stabilt og feilfritt.

Vi har brukt ordet informasjonssikkerhet i formuleringen av det første delproblemet. Informasjonssikkerhet deles ofte inn i fire hovedområder: autentisering, konfidensialitet, integritet og tilgjengelighet. Disse fire områdene henger nøye sammen når egenskaper innen sikkerhet skal beskrives. Det er vanskelig å oppnå sikkerhet uten pålitelighet. Et sikkert system må også til en viss grad være robust, stabilt og feilfritt.

Videre har vi benyttet uttrykket sensitiv informasjon, og vi tenker da på informasjon som bare er tilgjengelig for personer med gjeldende sikkerhetsklarering. Dette er informasjon som ikke er ment for allmennheten.

1.5 Militær sikkerhetsstruktur

Det er naturligvis slik at den parten med mest informasjon om fienden har et overtak. Etterretning har alltid vært en viktig bidragsyter til informasjonsinnsamling, og det er herfra uttrykket militær sikkerhet kommer. Med sikkerhet menes å skjule eller passe på informasjon som kan være en nasjonal sikkerhetstrussel, hvis den er kjent av fienden. All informasjon er ikke like sensitiv, og det er derfor opprettet forskjellige sensitivitetsnivåer. Nivåene for Norge er ugradert, BEGRENSET, KONFIDENSIELT, HEMMELIG og STRENGT HEMMELIG, der ugradert er offentlig informasjon og STRENGT HEMMELIG er svært sensitiv informasjon.

Personer som jobber med sensitiv informasjon må sikkerhetsklareres. Dette fordi at informasjon ikke skal bli kompromittert av upålitelige personer. Klareringsnivået indikerer om personen er tiltrodd det aktuelle nivået. Jo høyere klareringsnivå en person har, dess mer tiltrodd er vedkommende. Forsvaret utøver også noe som kalles need-to-know-prinsippet. Need-to-know-prinsippet går ut på at personer ikke skal få tilgang til informasjon de ikke har bruk for. Jo færre personer som vet en hemmelighet, jo mindre er sjansen for at hemmeligheten lekker ut. Dette prinsippet gjelder all gradert informasjon.

For noen spesielle tilfeller er sensitivitetsnivåene konkretisert. Dette gjelder blant annet for atomvåpen, NUCLEAR SECRET, og NATO-materiell, NATO RESTRICTED. Det kreves autorisasjonsbevis og et tjenstlig behov for å få tilgang til disse nivåene.

2 Litteraturreview

2.1 Generelle krav til informasjonsbehandlingssystem

Samarati og Vimercati (2001) sier at for å sikre et informasjonsbehandlingssystem må en definere noen viktige krav. Dataene og ressursene skal beskyttes slik at de ikke blir uautorisert avslørt (konfidensialitet) eller ulovelig endret (integritet), og slik at systemet samtidig sikrer tilgjengeligheten til brukerne (tilgjengelighet). For å nå disse kravene må en kontrollere alle tilganger til et system og dets ressurser, samt sørge for at bare autoriserte brukere kan få tilgang til systemet. Denne prosessen går under navnet tilgangskontroll (Access Control). Samarati og Vimercati (2001) sier videre at utviklingen av et tilgangskontrollsystem trenger regler for å vite hvilken tilgang som skal kontrolleres. Utviklingsprosessen blir vanligvis utført med en flerfaset tilnærming, basert på følgende konsepter:

- Sikkerhetspolitikk:
  Definerer hvilke lover som skal brukes og hvilke mål den skal oppnå.
- Sikkerhetsmodell:
  Skaffer en formell presentasjon av sikkerhetspolitikken.
- Sikkerhetsmekanismer:
  Hardwarefunksjoner og softwarefunksjoner som blir brukt til å implementere sikkerhetspolitikken.

2.2 Tilgangskontroll

Det finnes tre dominante tilgangskontrollpolitikker, Discretionary Access Control (DAC), Mandatory Access Control (MAC) og Role-Based Access Control (RBAC). I DAC er aksessen basert på identiteten til den som har bedt om tilgang, og tillatelsen til personen som allerede har tilgang. Tilgangen kan bli gitt eller ikke gitt av eieren av ressursen. I MAC blir tilgangsavgjørelser tatt i henhold til sikkerhetspolitikk bestemt av sentrale myndigheter. I RBAC kommer tilgangen an på hvilken rolle brukeren har i systemet, og på hvilke tilganger som er gitt til ulike roller.

Tabell 1: Tilgangskontrollpolitikker med tilhørende modeller.

DAC	MAC	RBAC
Access Matrix (Lampson, 1971)	Bell-LaPadula (Bell & LaPadula, 1973)	NPD (Baldwin, 1990)
Clark-Wilson Model (Clark & Wilson, 1987)	Biba Integrity Model (Biba, 1977)	
Chinese Wall(Brewer & Nash, 1989)		

2.2.1 Discretionary Access Control

Den klassiske modellen basert på DAC er tilgangskontrollmatrisen til Lampson (1971). Autorisasjonsproblemet er her sett på som en stor global tilgangskontrollmatrise A, med rader som tilsvarer subjekter og kolonner som tilsvarer objekter. Hver matriseinngang A[i, j]

uttrykker rettighetene som er gitt til subjekt i, med hensyn til objekt j. Tabellen på neste side viser et eksempel på en tilgangskontrollmatrise. Systemet har to prosesser og to filer, og rettighetene er {Lese, Skrive, Utføre, Tilføye, Eie}.

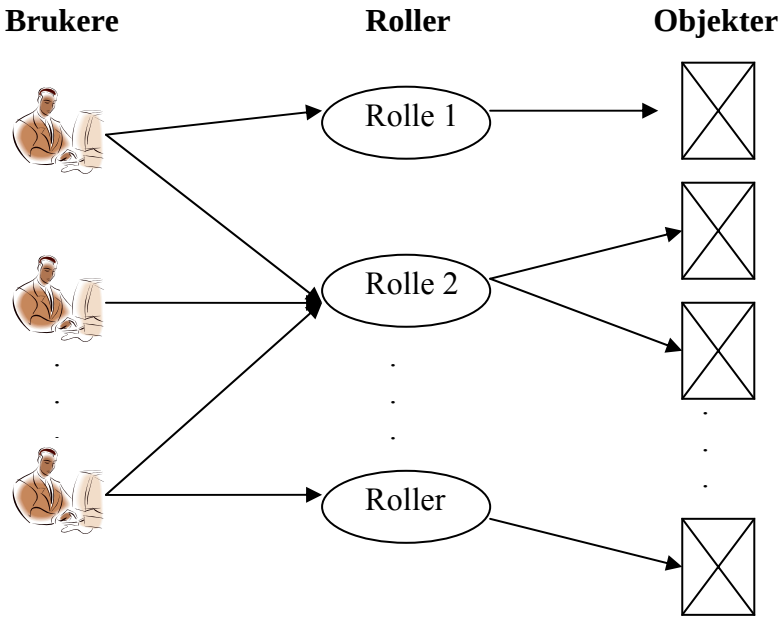
Tabell 2: Eksempel på tilgangskontrollmatrise.

	Fil 1	**Fil 2**	**Program 1**	**Program 2**
Gyda	Eie Lese Skrive	Lese	Eie Skrive Lese Utføre	Skrive
Per	Tilføye	Skrive Eie	Lese	Lese Skrive Utføre Eie

Hovedproblemet med DAC-modeller er ifølge Castano, Fugini, Martella og Samarati (1995), at spredningen av informasjon ikke er kontrollert. Dette gjør at DAC er svært sårbar for ondsinnede angrep som for eksempel trojanske hester. Trojanske hester er forklart i kapittel 3.2.1.

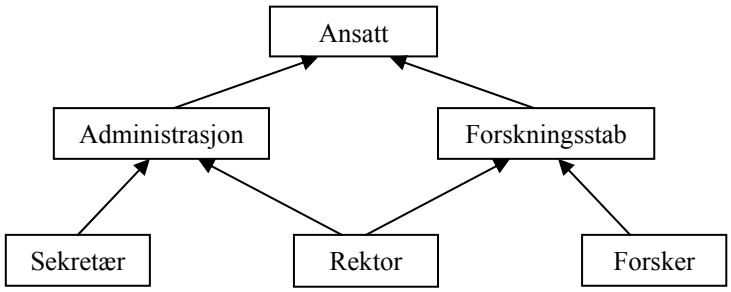
2.2.2 The Role-based Access Control Model

RBAC er et alternativ til DAC og MAC, og introduserer autentisering av roller. I virkeligheten kan en bruker ha forskjellige roller i forskjellige kontekster, selv om identiteten til brukeren forblir den samme. I følge Ren (2004) fanger en rollebasert tilgangsstyringsmodell opp dette konseptet naturlig ved å introdusere et ekstra nivå inn i normen for subjekt/objekt/rettighet, nemlig rolle. I stedet for å autentisere et subjekts tilgang til et objekt, blir autorisasjon uttrykt som en rolles adgang til et objekt, og subjektene kan bli tildelt ulike roller. Videre sier Ren (2004) at denne modellen letter administreringen av brukere, roller og tilganger. Den gjør det mulig å danne et rollehierarki, og den fremtvinger prinsipper som minste rettighet og deling av oppgaver. Modellen støtter mer justering og dynamiske restriksjoner enn vanlige tilgangsstyringsmodeller.



Figur 1: RBAC (Laget ut ifra Samarati & Vimercati, 2001).

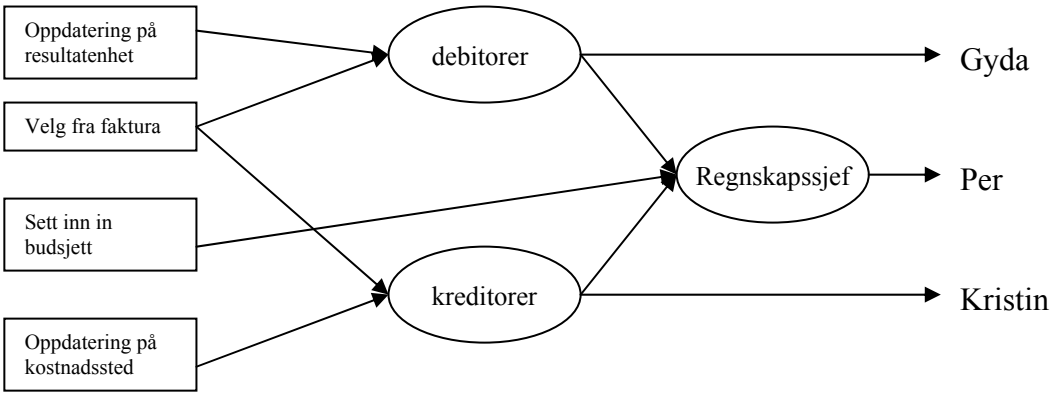
I mange sammenhenger er det et naturlig hierarki av roller, basert på familiære prinsipper for generalisering og spesialisering. Dette finner vi ofte innenfor ulike typer organisasjoner.



Figur 2: Rollehierarki.

Figuren over viser et svært enkelt hierarki der hver rolle er presentert ved en node. Videre går det en pil fra hver spesialisert rolle til dens generalisering. Med minste rettighet menes at ut ifra rolle, får brukeren tilgang med den laveste rettighet som trengs i en gitt situasjon. Personer som er autorisert for viktige roller, trenger ikke å benytte seg av disse rettighetene, før det faktisk er nødvendig. I følge Samarati og Vimercati (2001) minsker dette risikoen for nedsatt sikkerhet på nettet grunnet uoppmerksomhet fra brukerne, det minsker faren for trojanske hester og at uvedkommende får tilgang ved å utgi seg for å være legitime brukere. Videre sier Samarati og Vimercati (2001) at deling av oppgaver dreier seg om prinsippet at ingen brukere skal gis så høye rettigheter at de kan misbruke systemet på egenhånd. For eksempel skal ikke den personen som godkjenner en lønnsslipp, også være den som utarbeider den.

Named Protection Domain (NPD) av Baldwin (1990) er et eksempel på et konsept for RBAC. Dette er en måte å gjøre det enklere å administrere sikkerheten i et SQL-basert rammeverk. Et NPD identifiserer et sett med rettigheter som er nødvendige for å utføre en veldefinert oppgave. Samarati og Vimercati (2001) benytter et eksempel fra en bank for å vise dette. I en bank kan en NPD *debitor* defineres i forhold til de som har rettigheter som trengs for å utføre en debitor-oppgave. NPD kan gis til brukere så vel som til andre NPDer, og på denne måten danne en kjede av rettigheter. Autorisasjonstilstanden kan bli grafisk fremstilt som en styrt asyklisk graf, der noder tilsvarer rettigheter, NPDer og brukere, mens piler angir autorisasjonstildeling. Figur 3 viser et eksempel på en rettighetsgraf, som illustrerer tre NPDer med samsvarende rettigheter.



Figur 3: Eksempel på en NPD-rettighetsgraf (Laget ut ifra Samarati & Vimercati, 2001).

2.2.3 Mandatory Access Control

MAC-modeller er mindre brukt og strengere enn DAC-modeller. MAC-modellene kan forebygge både direkte og indirekte uheldig tilgang. De mest vanlige typene MAC-modeller jobber i et MLS-miljø, noe som er typisk for en militær setting. Den mest berømte MLS MAC-modellen er Bell-LaPadula (BLP) (Bell & LaPadula, 1973), som er en modell for konfidensialitet. Denne modellen omtales nærmere i 5.2.4.

En annen viktig MLS MAC-modell er Biba-modellen (Biba, 1977), som er en tilnærming til BLP-modellen (Bell & LaPadula, 1973). Den forbinder et integritetsnivå ved hver instans. Integritetsnivået består av et sett kategorier og en hierarkisk integritetsklassifisering. Klassifiseringen består av følgende tre verdier: Kritisk (K), Svært Viktig (SV) og Viktig (V), med K > SV > V.

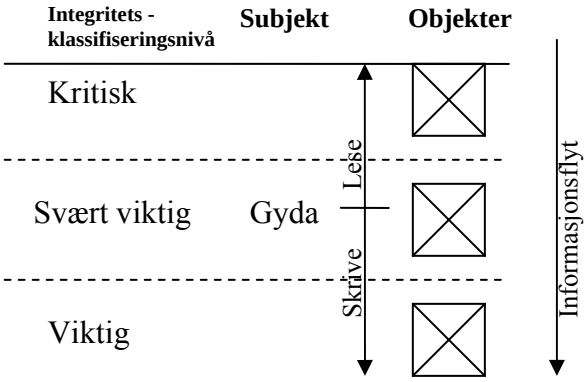
Et integritetsnivå L_1, sies å dominere integritetsnivå L_2, hvis:

1. Den hierarkiske klassifiseringen av L_1 er større enn eller er lik L_2 og
2. de ikke-hierarkiske kategoriene av L_1 inkluderer alle de av L_2 som en delmengde.

De to følgende reglene må bekreftes før et tiltak tillates:

1. Enkel integritetsegenskap (les-opp):
   Et subjekt kan bare få lesetilgang til et objekt, dersom subjektets integritetsnivå domineres av objektets integritetsnivå.
2. Integritetsstjerneegenskap (skriv-ned):
   Et subjekt kan bare få skrivetilgang til et objekt, dersom subjektets integritetsnivå dominerer objektets integritetsnivå.

Disse to tilstandene er forskjellige fra de uttrykt i BLP-modellen (Bell og LaPadula, 1973). Dette illustreres i figuren nedenfor. Gyda har integritetsklassifiseringsnivå *Svært Viktig*. I overensstemmelse med den enkle integritetsegenskapen kan hun ikke lese objekter som er *Viktig*. Videre kan hun på grunn av integritetsstjerneegenskapen, ikke skrive objekter som er *Kritisk*.



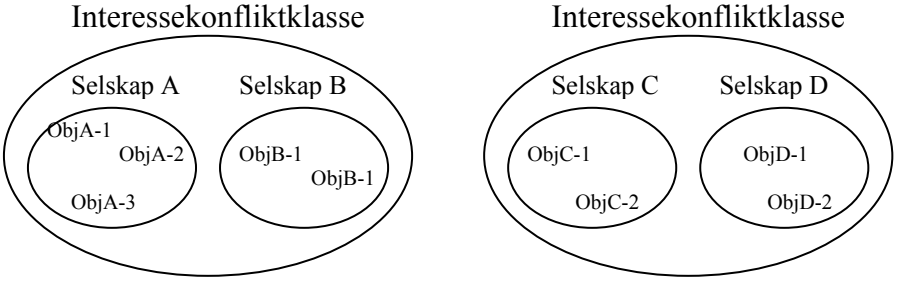
Figur 4: Informasjonsflyt i Biba-modellen (Laget ut ifra Samarati & Vimercati, 2001).

De to integritetsegenskapene er lette å forstå, dersom en betrakter integritetsnivået som et mål på hvor pålitelig informasjonen er. Dersom Gyda er klassifisert som *Svært Viktig*, og hun leser informasjon fra et *Viktig* dokument, betyr det at hun leser informasjon som er mindre pålitelig enn hennes eget integritetsnivå. Og hvis Gyda skriver i et *Kritisk* objekt, vil informasjonen i objektet bare ha pålitelighetsnivå *Svært Viktig*.

The Chinese Wall

Biba modellen (Biba, 1977) og BLP modellen (Bell & LaPadula, 1973) kommer begge fra en militær setting. Modellene jobber da i et statisk miljø, der sikkerhetsnivåene til subjektene og objektene forandrer seg lite. The Chinese wall (Brewer & Nash, 1989) kan sees på som en dynamisk modell, der objektene representerer forskjellige domener. Modellen er en hybrid mellom integritet og konfidensialitet, mens modellene til Biba og BLP er rendyrkede med henholdsvis integritet og konfidensialitet som egenskaper. Brewer og Nash (1989) samlet egenskapene integritet og konfidensialitet i en modell. Målet med modellen var å forebygge informasjonsflyter som laget interessekonflikter for de ulike konsulentene. Modellen baserer seg på en hierarkisk organisering av dataobjekter:

- *Grunnobjektene* er individuelle elementer av informasjon, der hvert element refererer til hver sin organisasjon.
- *Selskapdatasettene* definerer grupper av objekter som referer til den samme organisasjonen.
- *Interessekonfliktklassene* definerer selskapers datasett som referer til konkurrerende selskaper



Figur 5: Eksempel på The Chinese Wall (Laget ut ifra Brewer & Nash, 1989).

I figuren over har vi fire organisasjoner, Selskap A, B, C og D, med hvert sitt tilhørende *datasett for selskapet*. Disse har til sammen ni *Grunnobjekter*. Det er definert to *Interessekonfliktklasser*, henholdsvis mellom selskap A og B, og mellom selskap C og D.

2.2.4 Sikkerhetsmekanismer

Frem til nå har vi presentert aksesskontrollsystemer, sikkerhetspolitikker samt modeller fra litteraturen. I kapitlet om sikkerhetsmekanismer har vi presentert noen få pågående og ferdige prosjekter, der det er brukt forskjellige mekanismer for å oppnå modellstruktur og sikkerhetspolitikk.

Det har tidligere blitt skrevet at MLS-politikken modnet på begynnelsen av åttitallet. På slutten av åttitallet begynte de første MLS-operativsystemene å komme, og etter hvert ble MLS-konsepter utvidet til alle produkttyper.

SCOMP

The Secure Communications Processor (SCOMP) ble lansert i 1983, og var et produkt som det amerikanske forsvarsdepartementet ønsket for å kunne håndtere meldingsformidling på flere nivåer. I følge Anderson (2001) hadde SCOMP formelt sett verifisert hardware og software med en minimal kjerne og fire ringer med beskyttelse, for å gjøre ting enkelt. Operativsystemet, STOP, brukte disse ringene for å opprettholde opp til 32 separate felter, og for å tillate passende enveis informasjonsflyt mellom disse.

SCOMP ble i følge Anderson (2001) brukt i applikasjoner som militære mail guards, spesialiserte brannmurer som typisk tillater post å gå fra lavt til høyt nivå, men ikke omvendt. Etterfølgeren til SCOMP heter XT-300 og støtter the Command and Control Guard (C2G).

Dette blir brukt i systemet the Time-Phased Force Deployment Data (TPFDD) som har til oppgave å planlegge amerikanske troppers bevegelser og logistikk. I Anderson (2001) står det videre at militære planer overalt blir utviklet som TPFDD-er på et høyt klassifiseringsnivå, for deretter å bli distribuert på egnet tidspunkt til lavere nivåer for implementering.

SCOMPs mest betydningsfulle bidrag var å fungere som en modell for the Orange Book, også kalt TCSEC. Dette var, som nevnt tidligere, det første systematiske settet med standarder for sikre datasystemer.

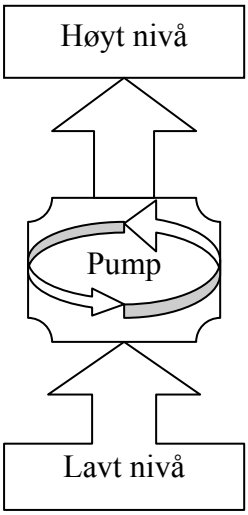
Blacker

Blacker kom på markedet i 1989 og var en serie med krypteringsanordninger designet for å innlemme MLS-teknologi. Tidligere ble krypteringsanordninger bygd med separate prosessorer for kryptogrammet (Black) og klarteksten (Red) (Anderson, 2001). Flere mulige feil kan forhindres hvis man kan koordinere Red og Black prosessering. Man kan også lage en enklere anordning og skaffe større operasjonell fleksibilitet. Anordninger er ikke begrenset til to atskilte logiske nettverk, men kan skaffe kryptering og integritetssikkerhet selektivt, og samhandle effektivt med rutere. I henhold til Anderson (2001) er et høyt sikkerhetsnivå påkrevd slik at Red data ikke lekker ut via Red.

I følge Anderson (2001) var den viktigste lærdommen fra Blacker, den ekstreme vanskeligheten med imøtekommende administrativ trafikk innenfor en modell med klassifiseringsnivåer. Så sent som i 1994 var dette den eneste kommunikasjonssikkerhetsanordningen med en A1-evaluering i henhold til TCSEC. Blacker hadde innvirkning på senere systemer, selv om den ikke ble brukt i stor utstrekning. Etterfølgeren, the Motorola Network Encryption System, er fortsatt i bruk, men denne har bare en B2-evaluering i henhold til TCSEC.

The NRL Pump

Enkle mail guards og kryptopostbokser ble altfor restriktive da en mengde nettverkstjenester kom på markedet for noen år tilbake. Tradisjonelle MLS-mekanismer som for eksempel lukket skriv-opp og periodisk les-ned, er ineffektive for sanntidstjenester. Av den grunn ble The NRL Pump utviklet ved The US Naval Research Laboratory (NRL) i 1996. Kang, Moskowitz og Lee (1996) skriver i sitt arbeid at pumpen er en enveis dataoverførselsanordning som bruker bufring for å tillate enveis informasjonsflyt. Samtidig begrenses båndbredden for mulige lekkasjer bakover med flere mekanismer, for eksempel uregelmessige tidsintervaller mellom sending av kvitteringsmeldinger (Kang et al., 1996).



Figur 6: The NRL Pump.

Denne metoden har gjort det mulig å lage MLS-systemer ved å bruke pumper for å knytte separate systemer til forskjellige sikkerhetsnivåer. Siden disse systemene ikke prosesserer data til mer enn ett nivå, kan de lages av rimelige, kommersielle og lett tilgjengelige lagerkomponenter (Kang et al., 1996).

I følge Anderson (2001) finnes det et australsk produkt kalt Starlight, som benytter pump-teknologien tilknyttet en tastatur-switch for å skaffe et MLS-Windowsbasert system. Ved å bruke tiltrodd hardware knyttes tastatur og mus opp mot høynivås og lavnivås systemer.

Purple Penelope

Standardapplikasjoner som MS Office er ikke anvendelige for de fleste MLS-plattformer. De blir likevel foretrukket av de fleste brukere, og Purple Penelope er en løsning for dette. Purple Penelope er utviklet for Ministry of Defence (MoD) i Storbritannia, som en del av The InfoSec Research Program. Denne setter en MLS-innpakning med tilhørende DAC-etiketter og tiltrodde stier, rundt en Windows NT arbeidsstasjon, som er evaluert i CC til Evaluation Level (EAL) 4. MLS-innpakningen viser det aktuelle sikkerhetsnivået for innretningen i bakgrunnen, og oppgraderer den når det er nødvendig ettersom mer sensitive ressurser leses. Dette sikrer at det resulterende arbeidet blir merket riktig.

I stedet for å beskytte brukerne mot nedgradering, tillater Purple Penelope at brukerne selv fastsetter sikkerhetsnivået på det de lager. Hvis dette involverer en nedgradering, må brukeren i følge Anderson (2001) bekrefte frigivelsen av data ved å bruke et sikkert grensesnitt, og på denne måten forsikre seg om at ingen trojanske hester eller virus kan frigi noe informasjon ubemerket. Et virkelig bra ondsinnet program kan likevel få med seg gradert materiell som brukeren ikke vil frigi, men det finnes et revisjonsspor for kopiering av alle nedgraderinger, slik at feil og angrep kan spores etter hendelsen.

I dag er Purple Penelope kommersialisert under QinetiQ og selges under navnet SyBard. SyBard utgjør i dag en del forskjellige komponenter, for eksempel en brannmurkomponent kalt for SWIPSY. Denne er evaluert i ITSEC til E3. Ifølge Simon Wiseman (personlig kommunikasjon, 28.april 2005) holder QinetiQ på med å planlegge en CC-evaluering av SyBard til EAL4. Grunnen til at de ikke sikter høyere, er at mekanismene til Windows ikke har høyere tiltro enn EAL4.

Miró

Miró-språkene og Miró-verktøyene er visuelle midler for å spesifisere filsystemsikkerhet (Heydon, 1990). Sikkerheten for filsystemet er modellert og uttrykt som en samling av brukere, en samling av filer og en samling av ulike tilgangsmetoder. Miró-miljøet har utviklet to visuelle spesifikasjonsspråk. Instansspråket spesifiserer tilgangsrettigheter for bestemte brukere til bestemte filer, og restriksjonsspråket spesifiserer restriksjoner til ulike fremgangsmåter som er tillatt.

Logisk baserte språk

Det har i den siste tiden vært en økning i bruk av logisk baserte språk til å implementere sikkerhetspolitikk. I følge Samarati og Vimercati (2001) er det første arbeidet med å kartlegge bruk av logisk baserte språk til å spesifisere autorisasjon, prosjektet til Woo og Lam (1993). De sier at det er et klart behov for fleksibilitet og tøyelighet i tilgangsspesifikasjoner. Woo og Lam (1993) viser videre hvordan en kan oppnå dette ved å bruke et høynivås autorisasjonsspråk. Språket er primært et førsteordensspråk uttrykt med ulike regler. Bruken av dette språket er svært generelt, da det har høy uttrykksstyrke, hvilket gjør at det er lett å uttrykke forskjellige autorisasjonsimplikasjoner, bundne autorisasjoner og tilgangskontrollregler.

Unified Modeling Language

Unified Modeling Language (UML) er et annet modelleringsspråk som er mye brukt i forbindelse med utvikling av sikkerhetsdesign. UML er et språk som kan spesifisere, lage og dokumentere ulike softwares med et visuelt uttrykk. UML har diagrammer som kan vise forskjellige perspektiver for ulike interessenter. Doan, Demurjian, Ting og Ketterl (2004) viser i sin artikkel hvordan de bruker UML til å adressere MAC. Videre fremlegger de noen sikkerhetsregler som sikrer sikkerhetsdominansen mellom nivåene. De bruker da UML til å fremlegge dette med diagrammer for use-cases, klasser og sekvenser. De presenterer ulike algoritmer som de implementerer i UML-diagrammene.

3 Multilevel Security

3.1 Introduksjon

For å få en et klart bilde av hva MLS er og innebærer, vil vi i dette kapittelet gi en innføring i MLS.

3.1.1 Bakgrunn

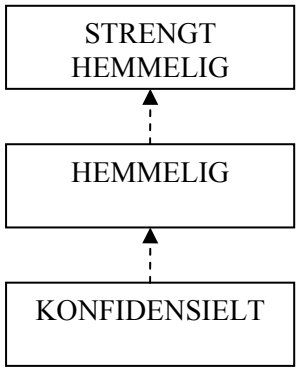
MLS har i følge Smith (2005) vært en utfordring innen datasikkerhet siden sekstitallet. MLS lyder som et ordinært problem innen tilgangsstyring: "*Allow information to flow freely between recipients in a computing system who have appropriate security clearances while preventing leaks to unauthorized recipients*" (Smith, 2005, Abstract).

MLS-systemer inkorporerer i følge Smith (2005) to nødvendige kjennetegn. For det første må systemet tvinge frem restriksjonene uansett tiltak fra systembrukere eller administratorer, og for det andre strever MLS-systemer for å håndheve restriksjonene med utrolig høy pålitelighet. Dette har fått utviklere til å implementere spesialiserte sikkerhetsmekanismer, og å legge til avanserte teknikker for å overprøve, analysere og teste mekanismene for riktig og pålitelig atferd. På tross av dette har MLS-systemer i følge Smith (2005), sjeldent skaffet den graden av sikkerhet som har vært ønsket av de mest krevende kundene i militære tjenester, etterretningsorganisasjoner og andre relaterte virksomheter. De høye kostnadene tilknyttet utvikling av MLS-produkter, kombinert med den begrensede mengden av brukere, har også vært med på å hindre MLS-funksjonaliteter i å komme fram i kommersielle produkter.

Mange firmaer og organisasjoner har behov for å beskytte hemmelig informasjon, og de fleste kan tolerere noe lekkasje. I forsvarssammenheng kan det imidlertid være svært vanskelig å komme på fote igjen etter sikkerhetsinformasjonslekkasjer. Et systems svakhet oppdages kanskje ikke før en diplomatisk eller militær katastrofe avslører den. I løpet av den kalde krigen ledet trusselen om nukleær tilintetgjøring, militære og politiske ledere til å ta slike risikoer veldig alvorlig. Det var lett å argumentere for at datalekkasje kunne true en nasjons eksistens. Nivåer for datasikkerhet ble etterspurt i forsvarssammenheng lenge før enn i annen virksomhet.

3.1.2 Sikkerhetsnivåer

Termen multilevel brukes fordi Forsvaret har klassifisert både mennesker og informasjon i ulike nivåer for sikkerhet og sensitivitet. Disse nivåene representerer sikkerhetsgraderingene KONFIDENSIELT, HEMMELIG, og STRENGT HEMMELIG. Disse nivåene former et hierarki som vist i figur 2. De stiplede pilene illustrerer i hvilken retning dataene kan gå, fra lavere nivåer til høyere nivåer, men ikke motsatt veg.



Figur 7: Hierarkiske sikkerhetsnivåer.

Det benyttes tre uttrykk i forbindelse med disse nivåene:

- Klareringsnivå: Indikerer nivået med tiltro gitt til en person med sikkerhetsklarering, eller en datamaskin som prosesserer gradert informasjon, eller et område som har vært fysisk sikret for lagring av gradert informasjon. Nivået indikerer det høyeste nivået med gradert informasjon som kan lagres eller håndteres av personen, innretningen eller lokasjonen.
- Graderingsnivå: Indikerer sensitivitetsnivået som assosieres med informasjonen i et dokument eller i en datafil. Nivået er ment å indikere graden av skade nasjonen kan påføres dersom en fiende avslører informasjonen.
- Sikkerhetsnivå: Er en generell terminologi for enten et klareringsnivå eller et graderingsnivå.

En sikkerhetsklarering gir ikke fullstendig tillatelse til å se på all informasjon gradert på gjeldende nivå eller lavere. Klareringen er bare første steg i fasen; personer får kun lov til å se på informasjon som er nødvendig for å utføre den jobben de er satt til å gjøre. En person som er sikkerhetsklarert for HEMMELIG for å jobbe med krypteringsinnretninger, har ikke tillatelse til å studere HEMMELIG informasjon om spionsatellitter. Dersom vedkommende jobber på et system som inneholder HEMMELIG informasjon om andre ting enn kryptografiske innretninger, må systemet beskyttes slik at denne personen ikke kan få tak i informasjon om andre prosjekter og aktiviteter. På den annen side må systemet kunne gi vedkommende tillatelse til å se på annet materiale. Dersom det er nødvendig for å utføre jobben. Dette er også kjent som need-to-know-prinsippet.

Forsvaret var i følge Smith (2005) den første og største kunden innen datateknologi, og datamaskinene var fortsatt veldig kostbare da de ble standardinnretninger i forsvarsorganisasjonene. Det var uansett få organisasjoner som kunne tilby separate datamaskiner for å behandle informasjon på hvert ulikt nivå, så de måtte utvikle prosedyrer for å dele datamaskinene uten å lekke gradert informasjon til uklarerte brukere. Dette var ikke så enkelt som først antatt. Følgelig anskaffet noen egne datamaskiner for å åpne utelukkende høyt gradert arbeid, uansett kostnad, bare fordi de ikke ville risikere informasjonslekkasje. I følge Smith (2005) gjorde flerbrukersystemer som de tidligere tidsdelingssystemene slik

deling særlig utfordrende. Ideelt sett kunne personer med sikkerhetsklarering jobbe samtidig som andre jobbet på STRENGT HEMMELIGE data, og alle skulle kunne dele like programmer og ugraderte filer. Mens typiske operativsystemmekanismer vanligvis kunne beskytte ulike brukerprogrammer fra hverandre, kunne de ikke beskytte en KONFIDENSIELL eller HEMMELIG bruker fra å lure en STRENGT HEMMELIG bruker, til å frigi STRENGT HEMMELIG informasjon via en trojansk hest.

3.1.3 Operasjonsmåter

Forsvaret beskriver vanligvis et flerbrukersystem ut fra operasjonsmåte. Sikkerhetsloven (2001) beskriver operasjonsmåtene som følger:

- Dedikert operasjonsmåte: *Når alle brukere er autorisert for all informasjon på informasjonssystemet og alt tilknyttet utstyr er godkjent for høyeste sikkerhetsgrad i systemet* (Sikkerhetsloven, 2001, § 5-2).
- Fellesnivå operasjonsmåte: *Når alle brukere er sikkerhetsklarert for høyeste sikkerhetsgrad i systemet, men ikke alle er autorisert for all informasjon på systemet, og alt tilknyttet utstyr og forbindelser er godkjent for høyeste sikkerhetsgrad i systemet* (Sikkerhetsloven, 2001, § 5-2). Et slikt system må ha mekanismer for å begrense brukernes tilgang. Dette krever typiske filaksessmekanismer for typiske flerbrukersystemer.
- Flernivå operasjonsmåte: *Når det er informasjon gradert KONFIDENSIELT eller høyere i systemet, og det er tilknyttet utstyr eller forbindelser som ikke er godkjent for høyeste sikkerhetsgrad i systemet eller det er brukere som ikke er klarert for høyeste sikkerhetsgrad i systemet* (Sikkerhetsloven, 2001, § 5-2). Systemet må ha en aksesskontrollmekanisme som håndhever MLS-restriksjoner.

En datamaskins operasjonsmåte bestemmer i følge Smith (2005) hvilke tilgangskontrollmekanismer som er nødvendig. Dedikerte systemer trenger kanskje ikke andre mekanismer enn fysisk sikkerhet. Maskiner som kjører fellesnivå operasjonsmåte må ha brukerbaserte tilgangsrestriksjoner. I flernivå operasjonsmåte må systemet beskytte data fra høyere nivåer mot lekkasje til brukere med lavere klarering; dette krever en spesiell mekanisme.

3.1.4 MLS-mekanismer

En MLS-mekanisme virker som følger: Brukere, datamaskiner og nettverk har etiketter som indikerer sikkerhetsnivåer. Data kan flyte fra samme nivå til samme nivå, eller fra lavere nivå til høyere nivå. På denne måten kan STRENGT HEMMELIGE brukere dele data med hverandre, og en STRENGT HEMMELIG bruker kan motta informasjon fra en HEMMELIG bruker. Det tillates ikke at data fra STRENGT HEMMELIGE brukere flyter inn i en fil eller andre lokasjoner som er synlig for en HEMMELIG bruker.

En direkte implementering av et slikt system tillater en forfatter av en STRENGT

HEMMELIG rapport å gjenopprette informasjon som er lagt inn av brukere på HEMMELIG eller KONFIDENSIELT, og integrere denne med STRENGT HEMMELIG informasjon. Brukeren med HEMMELIG klarering kan ikke lese det STRENGT HEMMELIGE resultatet, siden dataene bare flyter i en retning mellom HEMMELIG og STRENGT HEMMELIG. Ugraderte data kan gjøres synlige for alle brukere. Det er ikke tilstrekkelig å bare beskytte brukere med lavere klarering fra å lese data med høyere gradering. Hva om en bruker med STRENGT HEMMELIG klarering lagrer noen STRENGT HEMMELIGE data i en fil som kan leses av en HEMMELIG bruker? Dette lager det samme problemet som med å lese opp, siden det gjør STRENGT HEMMELIGE data synlige for HEMMELIGE brukere. Noen argumenterer med at STRENGT HEMMELIGE brukere bør bli tiltrodd å ikke gjøre sånne ting. Andre sier at de aldri vil gjøre det på grunn av at det er brudd på reglementer vedrørende spionasje. Dessverre tar ikke dette argumentet høyde for faren med trojanske hester.

3.2 Sikkerhetsutfordringer

3.2.1 Trojanske hester

En trojansk hest er software med en usynlig og ødeleggende funksjon. I et flerbrukersystem kan brukere lagre private filer og bruke systemets tilgangstillatelse for å beskytte disse filene. Det kan tenkes at en nysgjerrig bruker utvikler et lokalt ordprosesseringsprogram for å få innsyn i de andre brukernes beskyttede filer. Han kan da installere en trojansk hest funksjon i ordprosesseringsprogrammet for å finne igjen de beskyttede filene. Funksjonen kopier så de andre brukernes private filer inn i vedkommendes eget register hver gang noen kjører ordprosesseringsprogrammet. Når en bruker kjører et ordprosesseringsprogram, arver programmet denne brukerens tilgangstillatelser til brukerens egne filer. Slik omgår den trojanske hesten tilgangstillatelsene.

I følge Smith (2005), kan ikke et system håndheve MLS-tillit hvis trojansk hest programmer kan omgå MLS-beskyttelser. Videre er det ikke mulig for brukere å unngå trojansk hest programmer med hundre prosent pålitelighet. En effektiv MLS-mekanisme må kunne blokkere forsøk på å skrive ned, så vel som forsøk på å lese opp (Smith, 2005).

3.2.2 Skjulte kanaler

Lampson publiserte i 1973 en artikkel om et problem kjent som The Confinement problem. Problemet oppstår når et program har tilgang til graderte data på vegne av en prosess. Det som da kan skje er at programmet kan lekke ut informasjon til andre prosesser eller filer i datasystemet. Lampson (1973) identifiserer tre typer av kanaler som kan bli brukt til å lekke informasjon.

Lovlige kanaler blir brukt til å transportere resultatene av en beregning. Det er i følge Lampson (1973) mulig å skjule informasjon i disse kanalene ved å variere linjeavstanden, og på denne måten kan høyere gradert informasjon komme ned på et lavere gradert nivå.

Lagringskanaler er de kanalene som sender data fra en høy prosess til en lav prosess ved å skrive data til en lagringsplass, som er synlig for den lave prosessen. Det er da mulig å lagre høyere gradert informasjon på disse lagringsplassene via lagringskanalene.

Den siste kanalen som kan lekke informasjon er Tidskanalen. Tidskanalen varierer tiden mellom oppgavene når en høy prosess kommuniserer med en lav prosess. Et eksempel på en kommunikasjon mellom en høy og en lav prosess, er hvis en høy prosess ber en harddisk om å aksessere noen høyere graderte blokker, samtidig som en lav prosess skal ha noen lavere graderte blokker på den samme harddisken. Den lave prosessen vil da få en tidsforsinkelse på grunn av aktiviteten til den høye prosessen. Denne tidsforsinkelsen lager et mønster for når den lave prosessen kan motta høyere gradert informasjon.

3.2.3 Begrensninger i Multilevel Security -systemer

På tross av støtte fra forsvarsmiljøer og stor innsats fra data- og programvareleverandører, samt forskere innen datasikkerhet, har ikke MLS-mekanismene klart å skaffe den sikkerheten og funksjonaliteten som forsvarene krever. Et av problemene er at sikkerhetsforskere og systemutviklere innen MLS har funnet det svært vanskelig, eller umulig, å totalt beskytte informasjonsflyt mellom ulike sikkerhetsnivåer i et MLS-system. Et annet problem er virustrusselen, da en med MLS-informasjonsflyt ikke klarer å beskytte et virus som har blitt introdusert på et lavere klareringsnivå fra å spres til høyere klareringsnivåer. Et tredje problem er at BLP-baserte systemer har en tendens til å samle en mengde overgradert informasjon. Når en bruker lager et dokument på et høyt sikkerhetsnivå, må dokumentet holdes på dette nivået, selv om brukeren fjerner all sensitiv informasjon for å lage et lavere gradert eller ugradert dokument. I hovedsak trenger brukerne ofte en mekanisme for å nedgradere informasjonen. I praksis vil systemer løse dette problemet ved å installere privilegerte programmer som omgår MLS-mekanismen for å nedgradere informasjon.

3.2.4 Tillitsproblemet

Allerede på sekstitallet identifiserte forsvarsmiljøene behovet for MLS-systemer, og noen få leverandører implementerte basismomentene. Studier innen MLS viste imidlertid farer ved å stole på store, ugjennomskinnelige operativsystemer for å beskytte hemmelig informasjon. Operativsystemer var allerede beryktet for upålitelighet, og disse studiene belyste trusselen av softwarefeil som tillater lekkasje av høyt gradert informasjon. Den anbefalte løsningen var å oppnå høy tiltro gjennom omfattende analyser, betraktninger og testing. Selv om høy tillit ville øke leverandørers utviklingskostnader og føre til høyere produktkostnader, avskrekket ikke dette det amerikanske forsvaret som forutså langtids kostnadsinnsparinger.

Smith (2005) påpeker et fundamentalt spørsmål vedrørende MLS-innretninger: Håndhever systemet MLS, eller lekker det informasjon på noen måte? Problemet kan deles inn i ytterligere to spørsmål: Hva menes egentlig med å håndheve MLS? Og hvordan kan man evaluere et system for å verifisere at det håndhever MLS?

Det første spørsmålet ble i følge Smith (2005) besvart med utviklingen av sikkerhetsmodeller, slik som BLP. En formell modell gjør håndhevingsproblemet klart for ikke-programmerere, og synliggjør også driftskravene overfor programmererne som implementerte MLS-mekanismene. Det andre spørsmålet ble i følge Smith (2005) besvart med utviklingen av to sett med strategier for å evaluere MLS-systemer. Det første var strategier for å designe et pålitelig MLS-system, og det andre var strategier for å bevise at MLS-systemene virker korrekt.

4 Metode

4.1 Generelt

Sosiologen Vilhelm Aubert har definert metode som: ”… *en framgangsmåte, et middel til å løse problemer og komme fram til ny kunnskap. Et hvilket som helst middel som tjener dette formålet, hører med i arsenalet av metoder*.” (Dalland, 2000).

Når en snakker om metode, er det vanlig å skille mellom to typer; kvalitative og kvantitative metoder. Kvalitativ metode innebærer i følge Olsson og Sørensen (2003) at en stiller med blanke ark, og prøver å møte situasjonen som om den alltid har vært ny og å strebe etter en helhetsforståelse av spesifikke formål. Videre er det sentrale med kvalitativ tilnærming å prøve å komme frem til de kategorier, beskrivelser eller modeller som best beskriver et fenomen (Olsson & Sørensen, 2003). Med kvantitativ metode menes: *"framgangsmåter der forskeren først systematisk skaffer seg sammenlignbare opplysninger om flere undersøkelsesobjekter av et visst slag, så uttrykker disse opplysningene i form av tall, og til slutt foretar en analyse av mønsteret i dette tallmaterialet."* (Hellevik, 1991).

4.2 Metodisk tilnærming

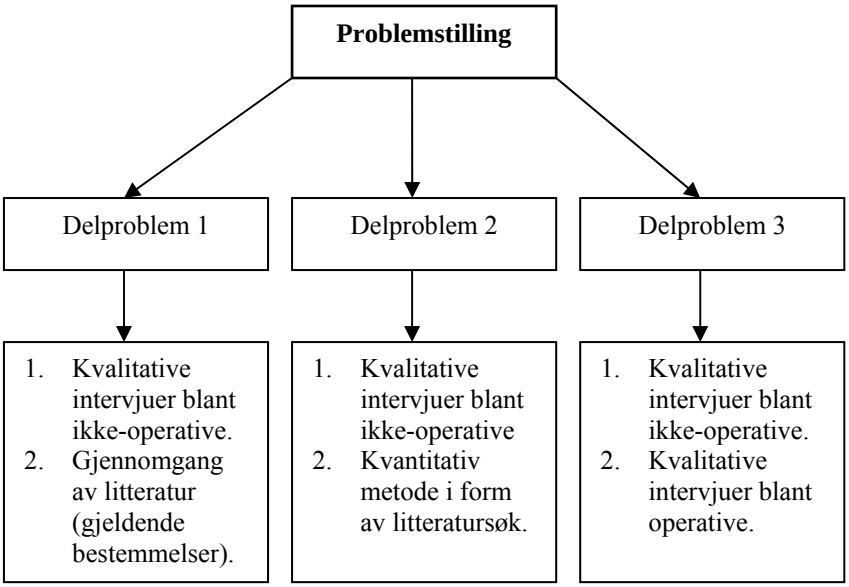
Problemstillingen vår gikk ut på å kartlegge situasjonen innenfor MLS og redegjøre for teorier og strategier på området, og på grunnlag av dette, vurdere ulike løsninger for Forsvaret. Dette var en forholdsvis bred problemstilling, og vi valgte å tilnærme oss den ved å lage tre, mer spesifikke, delproblemer. Disse ble svært forskjellige, og vi har derfor benyttet ulike metoder for å tilnærme oss problemstillingene. En slik kombinasjon av kvalitativ og kvantitativ metode, kalles metodetriangulering (Johannessen, Kristoffersen & Tufte, 2004).

Det første delproblemet var å systematisere Forsvarets krav til systemer som sammenkobler informasjon med ulik sikkerhetsgradering. Dette krevde at vi fikk tilgang til gjeldende lover og regler innen informasjonssikkerhet, og at vi deretter gikk nøye gjennom innholdet og systematiserte dette. For å lette arbeidet noe, valgte vi å gjennomføre kvalitative intervjuer med personer som jobber innen sikkerhet og IKT i Forsvaret.

Det andre delproblemet var å redegjøre for teorier og strategier innen MLS, samt å presentere realiserte MLS-systemer. Vi benyttet en kvantitativ tilnærming med et omfattende litteratursøk. Deretter måtte informasjonen systematiseres, og vi måtte foreta en utvelgelse av spesifikke teorier og modeller. Videre i denne prosessen valgte vi å gjennomføre kvalitative intervjuer; først og fremst for å få innspill om realiserte MLS-systemer.

Det tredje og siste delproblemet gikk ut på å utrede konsekvensene av innføringen av et system som sammenkobler informasjon med ulik sikkerhetsgradering. Dette krevde innspill

fra personer med erfaring fra å jobbe med og på systemer med gradert informasjon. Vi valgte derfor å gjennomføre to intervjurunder. Først ble det foretatt en kvalitativ undersøkelse blant personell som jobber med sikkerhet og IKT i Forsvaret, og deretter ble det gjennomført en annen kvalitativ undersøkelse blant operativt personell som jobber på graderte systemer til daglig.



Figur 8: Metodisk tilnærming.

Videre følger en nærmere beskrivelse av den metodiske tilnærmingen til hvert delproblem. Deretter har vi beskrevet de to kvalitative undersøkelsene, først den som benyttes i alle delproblemene, og deretter den som gjelder for det tredje delproblemet.

4.3 Tilnærming for hvert delproblem

Nedenfor har vi beskrevet metodetilnærmingen for hvert enkelt delproblem. Siden intervjuene dekker flere delproblemer, har vi valgt å omtale disse for seg.

4.3.1 Delproblem 1

Det første delproblemet var å systematisere Forsvarets krav til systemer som sammenkobler informasjon med ulik sikkerhetsgradering.

Alternative metoder

Uansett valg av metode, måtte vi først finne ut hvilke regelverk Forsvaret må forholde seg til, for deretter å gå inn og finne spesifikke paragrafer vedrørende systemer som sammenkobler informasjon.
En måte å gjøre dette på kunne ha vært å søke direkte på Internett for å finne frem til gjeldende lovverk. Dette kunne ha tatt mye tid, samtidig som vi sannsynligvis ville ha fått opp mye irrelevant informasjon.

Etter å ha funnet frem til gjeldende lovverk, kunne vi ha satt oss ned og lest alle dokumentene for om mulig å finne frem til relevante punkter vedrørende MLS. Dette anså vi som en altfor tidkrevende og vanskelig oppgave. Sikkerhetsloven med forskrifter og veiledninger er svært omfattende.

Det var mer nærliggende å kontakte NSM som er ansvarlig for å håndheve og tolke den nasjonale sikkerhetsloven. Høyst sannsynlig har NSM også mye kunnskaper vedrørende internasjonale lover og regler som Forsvaret må forholde seg til, blant annet bestemmelser gitt av NATO. Gjentatte forsøk på å få til en avtale med NSM, både på egenhånd og med hjelp fra teknisk veileder, lyktes imidlertid ikke.

Det alternativet vi sto igjen med var å kontakte personer som jobber med sikkerhet i Forsvaret, og få hjelp av dem til å finne fram til gjeldende bestemmelser. Spørsmålet var hvordan vi skulle hente denne informasjonen; ved å ringe og spørre tilfeldige personer i ulike sikkerhetsavdelinger, eller ved å utarbeide en noe mer omfattende undersøkelse med godt forberedte spørsmål. Vi valgte det siste alternativet.

Valgt metode

Gjennom vår tekniske veileder fikk vi rede på hvilke lover som er styrende. På Internett fant vi blant annet Sikkerhetsloven med forskrifter og veiledninger. Lovverk fra NATO er imidlertid graderte dokumenter og er ikke tilgjengelige.

Det viste seg noe vanskelig å finne fram i Sikkerhetsloven med forskrifter og veiledninger på egen hånd; primært fordi vi ikke kjente til hvilke deler som har innvirkning på sammenkobling av systemer med ulik gradering.

Vi hadde tidligere avtalt intervjuer med personell innen sikkerhet og IKT i Forsvaret i forbindelse med de øvrige delproblemene. Følgelig bestemte vi oss for å innlemme spørsmål vedrørende gjeldende sikkerhetskrav i disse intervjuene. Spørsmålene står i intervjuguiden, vedlegg A, og resultatene er gjengitt i vedlegg B.

I tillegg til å gjennomføre undersøkelsen, kontaktet vi programsikkerhetsavdelingen i Program Golf. Der snakket vi med programsikkerhetsleder oberstløytnant Tom Hvalby, som har vært med og utarbeidet interne dokumenter i Program Golf vedrørende FIF. Han har i denne forbindelse vært ansvarlig for å skrive delene om sikkerhet, og ga oss gode innspill til oppgaven. Videre tok vi også kontakt med et britisk datateknologifirma, QinetiQ, som har utarbeidet diverse MLS-løsninger. På grunn av dette har bedriften god kjennskap til gjeldende evalueringskriterier, og ga oss nyttig informasjon i denne forbindelse.

4.3.2 Delproblem 2

Det andre delproblemet var å redegjøre for teorier og strategier innen MLS, samt presentere realiserte MLS-systemer.

Alternative metoder

Vi hadde i forkant av problemformuleringen foretatt mange søk på Internett og i litteraturdatabaser vedrørende MLS. Vi visste derfor at det fantes uante mengder lett tilgjengelig informasjon rundt emnet.

Vi så for oss at det kunne bli vanskelig å finne fram i, og plukke ut den mest relevante informasjonen på egenhånd. Av den grunn vurderte vi i første omgang å gjøre en undersøkelse blant folk med spesiell kompetanse innen MLS. Det viste seg imidlertid svært vanskelig å finne personer i Norge, med spesiell kunnskap om MLS. Vi bestemte oss derfor for å stille spørsmål om teorier og strategier til ansatte innen sikkerhet og IKT i Forsvaret.

Alternativet, dersom vi ikke fikk noe ut av intervjuene, var å hente informasjon fra Internett og litteraturdatabaser, for så å gjennomgå og systematisere informasjonen på egenhånd.

Valgt metode

Som sagt endte vi opp med å gjennomføre en undersøkelse blant ansatte innen sikkerhet og IKT i Forsvaret, hvorav noen var inneleide konsulenter fra sivile bedrifter. Intervjuobjektene hadde alle gode kunnskaper innen sine fagfelt, men ikke uventet noe sprikende kunnskaper innen MLS-teori. Vi fikk flere gode inputs vedrørende MLS-systemer og nåværende løsninger i Forsvaret, men ingen visste nevneverdig mye om konkrete teorier og strategier som har versert de siste tiårene.

Vi måtte altså finne frem i informasjonsjungelen på egenhånd. Ved bruk av Internett, litteraturdatabaser og fagbøker fant vi en mengde informasjon. Vi gjennomgikk og systematiserte all informasjonen. Etter beste evne plukket vi ut modeller, strategier og teorier, som etter vårt syn presenterte de viktigste trendene innen MLS, fra starten og frem til nå.

4.3.3 Delproblem 3

Det siste delproblemet gikk ut på å utrede konsekvensene av innføringen av et system som sammenkobler informasjon med ulik sikkerhetsgradering.

Alternative metoder

Vi vurderte ulike måter å tilnærme oss dette problemet på. I første omgang hadde vi tenkt å studere erfaringer fra tidligere MLS-innføringer i ulike bedrifter. Dette finnes det imidlertid ikke mange eksempler på. Dessuten stiller Forsvaret betydelig høyere krav til sikkerhet og tiltro enn de fleste andre bedrifter. Eksempler på tidligere implementeringer var derfor ikke av spesielt stor relevans, og ville gi begrenset nytte i forhold til MLS i forsvarssammenheng.

Et annet alternativ var å gjennomføre intervjuer blant folk som har greie på hva en innføring av et MLS-system kan innebære for Forsvaret. Vi bestemte oss derfor for å intervjue folk som jobber med sikkerhet og IKT i Forsvaret. Dette er personer som fortrinnsvis jobber med utvikling, implementering, sikkerhetsforebyggende tiltak, diverse prosjekter og lignende.

Vi så for oss at dette kunne bli noe snevert uten synspunkter fra de som faktisk jobber på graderte systemer. Vi bestemte oss derfor for å gjennomføre ytterligere en spørreundersøkelse, men da blant operativt personell som jobber på graderte systemer til daglig.

Valgt metode

Vi hadde allerede avtalt intervjuer med forsvarsansatte innen sikkerhet og IKT, og valgte å få deres syn på hvilke konsekvenser som kan oppstå i forbindelse med en eventuell MLS-innføring i Forsvaret. Synspunktene deres var basert på erfaringer fra tidligere og eksisterende systemer i Forsvaret, innføringer av MLS-systemer i andre bedrifter, samt pågående arbeid med å finne nye og bedre løsninger for informasjonsflyt i Forsvaret. Intervjuobjektene vi her omtaler er alle ikke-operative, og har erfaringer fra å jobbe med, og ikke på, systemer med ulike graderinger.

For å få en bredere forståelse av hvordan nåværende systemer oppleves av de reelle brukerne, valgte vi som sagt å supplere med en undersøkelse blant operativt personell. Denne gruppen kunne gi oss inputs på hvordan det oppleves å jobbe på dagens løsninger for gradert informasjon i Forsvaret, og hvilke konsekvenser en eventuell MLS-innføring kan medføre for dem og deres arbeidssituasjon.

4.4 Kvalitative undersøkelser

For å få et godt intervjuresultat er en i følge Olsson og Sørensen (2003) nødt til å definere grundig så vel formål som problemområde før undersøkelsen starter. Videre bør undersøkelsens hvorfor og hva klargjøres før man stiller spørsmålet om hvordan. Delproblem en, to og tre er utgangspunktene for våre undersøkelser. Vi har valgt å gjennomføre i alt to kvalitative intervjurunder, der resultatene fra den første er benyttet i alle delproblemene, mens resultatene fra den siste er benyttet kun for å svare på delproblem tre.

I begge intervjurundene har vi benyttet strategisk utvelging av informanter. Strategisk utvelging innebærer at forskeren på forhånd har bestemt seg for hvilken målgruppe forskningen skal rette seg mot for å samle inn nødvendige data (Johannessen et al. , 2004). I første omgang gjennomførte vi personlige intervjuer med fem personer som jobber hovedsakelig med sikkerhet eller informasjons- og kommunikasjonsteknologi (IKT) i Forsvaret. I andre omgang gjennomførte vi intervjuer blant operativt personell i Forsvaret.

Intervjuene har bidratt til å gi oss en dypere forståelse av situasjonen vedrørende MLS i Forsvaret. Dette gjelder både hvordan dagens systemer fungerer i forhold til hvordan et MLS-system kan fungere, samt hvilke konsekvenser et MLS-system kan få for de ansatte. Videre har vi fått et innblikk i hvordan de ansatte forholder seg til tanken om innføring av MLS i det norske forsvaret.

4.4.1 Kvalitativ undersøkelse 1

Tilnærming

Den første intervjurunden ble basert på kvalitative intervjuer. Det vil si at vi stilte åpne spørsmål, slik at informantene kunne formulere svarene med egne ord. Dette ga oss en indikasjon på om informanten hadde forstått spørsmålet. Videre kunne de snakke fritt rundt hvert spørsmål, alt etter som hvor mye kunnskap de hadde om de ulike temaene.

Videre valgte vi å gjennomføre den første intervjurunden som semistrukturerte eller delvis strukturerte intervjuer. Vi benyttet en overordnet intervjuguide som utgangspunkt for intervjuet, hvilket ga oss mulighet til å variere spørsmål, temaer og rekkefølge underveis. Hovedårsaken til at vi valgte denne intervjumåten, var at informantene hadde ulike bakgrunner og dermed spesielle kunnskaper innen forskjellige områder. En intervjuguide ga oss muligheten til å få intervjuobjektene til å snakke om temaer som de kunne mye om.

Utforming av intervjuguide

En intervjuguide er en liste over temaer og generelle spørsmål som skal gjennomgås i løpet av intervjuet. Vi delte intervjuguiden, vedlegg A, inn i tre hovedtemaer basert på delproblemene i oppgaven.

Videre formulerte vi underspørsmål for å få utdypet de forskjellige temaene. Foran hvert spørsmål lagde vi en innledning for å gi en bakgrunn for hvorfor vi stilte de enkelte spørsmålene. Dette for å kvalitetssikre intervjuguiden for vår egen del, men også for å gi en informasjon til intervjuobjektene i tilfeller der de ikke forstod hva det ble spurt etter, eller ikke kjente til problemstillingen.

Det var svært viktig at undersøkelsen ga oss svar på det vi ønsket å finne ut av. Vi brukte derfor lang tid på å utforme relevante og gode spørsmål, og foretok en grundig analyse av hvilke spørsmål vi skulle ha med og hvorfor. Med gode spørsmål mener vi spørsmål som gir nyttige og fyldige svar.

Videre satte vi opp mulige svaralternativer under hvert spørsmål. Dette gjorde vi først og fremst for å gjøre det lettere å notere underveis. I tillegg hjalp dette oss til å sette i gang tankene hos intervjuobjektene i tilfeller der de trodde de ikke kunne svare. Dette erfarte vi spesielt i forbindelse med del to, kartlegging av MLS-teorier og strategier. I utgangspunktet

kjente ingen til noen MLS-modeller, men flere hadde hørt om modellene vi hadde satt opp som svaralternativer.

Utvalg

Vi ønsket å intervjue personer med spesiell kunnskap innen MLS, og helst med kjennskap til Forsvaret og dets systemer. Dette var et nytt og ukjent område for oss og vi oppsøkte derfor hjelp for å finne aktuelle intervjuobjekter. Med hjelp fra vår tekniske veileder i Program Golf, Hans Petter Egeland, kom vi i kontakt med flere personer som hadde spesiell kunnskap innen MLS eller tilhørende fagområder. Vi tok kontakt med de enkelte personene per telefon for å få greie på hva slags kunnskaper de hadde, og for å få rede på om de hadde anledning til å bli intervjuet.

Vi endte opp med et utvalg på fem personer som alle jobber eller har jobbet, i Forsvaret. Øyvind Nyquist er prosjektsikkerhetsleder FISBasis og Systemforvalter Tonivå og Sikkerhet, Øyvind Hvinden jobber i Forsvarets Logistikkorganisasjon (FLO)/IKT. Nicolay Nakstad er ansatt i Sentral Sikkerhetsgruppe, Program Golf. Det samme er Håkon Liberg, han er imidlertid innleid som konsulent fra IBM, men har uttalt seg som privatperson i undersøkelsen. Jon Ølnes kommer fra Det Norske Veritas, og har tidligere jobbet i IBM som konsulent i Program Golf.

Utførelse av intervjuene

I forkant av intervjuene snakket vi med hver enkelt og informerte om oppgaven og undersøkelsen. Videre sendte vi ut temaene og tilhørende spørsmål som e-post, slik at den enkelte skulle få mulighet til å være godt forberedt. Vi avtalte tid og sted for intervjuene på forhånd, og ba intervjuobjektene sette av minimum en time til gjennomføringen.

Da intervjuene skulle gjennomføres, visste den enkelte allerede hvem vi var og hva oppgaven gikk ut på. På denne måten sparte vi tid og kunne starte selve intervjuet forholdsvis raskt. Som forventet var det store forskjeller i hvor mye intervjuobjektene kunne om de ulike temaene. Det var viktig for oss å holde oss innenfor den fastsatte tiden, og vi måtte derfor i enkelte tilfeller styre intervjuobjektene, da de snakket utover de egentlige spørsmålene.

Behandling av data/ dokumentasjon

Hvert intervju hadde en varighet på om lag en time og ble gjennomført ved personlig fremmøte. Vi var begge to til stede ved samtlige intervjuer, den ene intervjuet mens den andre noterte.

Ellers benyttet vi med tillatelse fra intervjuobjektene, en mp3-spiller for å tape intervjuene. I etterkant skrev vi ned intervjuene ordrett, sammenliknet svarene med notatene, og sorterte deretter informasjonen etter tema. Til slutt samlet vi informasjonen i en skjematisk oversikt, se vedlegg B.

4.4.2 Kvalitativ undersøkelse 2

Tilnærming

Den andre intervjurunden skulle gi svar på det tredje delproblemet i oppgaven. I utgangspunktet hadde vi tenkt å gjennomføre denne intervjurunden på samme måte som den første. Det viste seg at det var vanskelig å gjennomføre dette, siden intervjuobjektene var spredd i inn- og utland. Intervjuene kunne ikke foretas per telefon på grunn av dårlig telefonforbindelse til flere av intervjuobjektene.

Vi ble følgelig nødt til å benytte skriftlig intervjuform, og baserte intervjurunden på strukturerte intervjuer med på forhånd fastlagte temaer og spørsmålsformuleringer. Videre kan intervjuene karakteriseres som standardiserte, det vil si at de var nøye planlagt uten mulighet til å variere situasjonen fra en intervjuperson til en annen (Olsson og Sørensen, 2003).

Utforming av spørreskjema

For å unngå misforståelser skrev vi opp definisjonen på MLS øverst på undersøkelsen. Dette for å gi intervjuobjektene en felles forståelse for hva MLS innebærer. Videre hadde vi som utgangspunkt at utfyllingen av skjemaet ikke skulle ta mer enn tretti minutter. Dette ble vi enige om etter å ha vært i kontakt med aktuelle intervjuobjekter, som ga uttrykk for at en halvtime var den maksimale tiden de ville avse for å svare på en slik undersøkelse.

I og med at vi ikke kunne utføre intervjuene personlig, måtte vi lage prekodede spørreskjemaer, vedlegg C, der en på forhånd må vite hva en skal spørre om. Dette krevde at vi var ekstra nøye med utarbeidelsen av spørsmålene, slik at de ville gi svar på det vi ønsket. Utvelgelsen av hvilke spørsmål som skulle være med eller ikke,var en omstendelig prosess. Videre la vi vekt på å lage presise formuleringer, slik at det ikke ble rom for misforståelser.

Undersøkelsen er bygd opp med innledende spørsmål først, dernest spørsmål vedrørende nåsituasjonen og arbeidet de utfører, og til slutt spørsmål om synspunkter angående MLS i fremtiden.

De fleste spørsmålene har faste svaralternativer, slik at intervjuobjektene kunne krysse av for svaret de mente passet best. Samtidig er de fleste spørsmålene åpne for merknader. I og med at spørreskjemaet er strukturert med svaralternativer, samtidig som det åpner for åpne og prestrukturerte svar, er det en semistrukturert undersøkelse.

Utvalg

I den andre intervjurunden ønsket vi å intervjue personer som jobber på ulikt graderte nett til daglig, fortrinnsvis med erfaring fra utenlandsoperasjoner med tilhørende NATO-nett. Personene ble forespurt ut ifra personlige kontakter og ”snøballmetoden”, det vil si at

informantene ble rekruttert ved at vi forhørte oss om hvilke personer som visste mye om det temaet som skulle undersøkes, og så kontaktet vi dem (Johannessen et al., 2004). Disse personene kjente igjen til andre informanter som kunne være aktuelle å ha med i undersøkelsen.

Vi opplevde mange negative responser på grunn av stort arbeidspress. Vi endte til slutt opp med et utvalg bestående av fire personer. Samtlige av disse jobber i Forsvarets spesialstyrker og ønsket av den grunn å være anonyme. Personene som deltok i den andre undersøkelsen omtales derfor som A, B, C og D.

Utførelse av intervjuene

Intervjuene ble som nevnt tidligere basert på skriftlige besvarelser, og utfyllingen var beregnet til å ta om lag tjue minutter. Intervjuene ble sendt ut og besvart via e-post. Samtlige av dem vi hadde avtalt intervju med, svarte på undersøkelsen.

Behandling av data/dokumentasjon

På grunn av ønsket om anonymitet, kategoriserte vi intervjuobjektene fra A til D. Vi samlet informasjonen fra de fire intervjuene og satte den inn i et samlet dokument, vedlegg D. I og med at antallet intervjuobjekter var såpass lite, ble dette svært oversiktlig og enkelt å benytte i det videre arbeidet.

5 Resultater

5.1 Delproblem 1: Gjeldende sikkerhetsbestemmelser

Vi skal systematisere Forsvarets krav til systemer som sammenkobler informasjon med ulik sikkerhetsgradering.

5.1.1 Bakgrunn

Full implementering av NbF vil kreve flernivå sikkerhetsfunksjonalitet, det vil si fullverdig MLS. Et fullverdig MLS-system har informasjonsflyt fra Internett til HEMMELIG. Dette krever tilgang på sertifiserte operativsystemer og applikasjoner med MLS-funksjonalitet samt høytillits brannmursystemer som samtidig tilfredsstiller krav til tiltro, funksjonalitet og fleksibilitet.

Nasjonal sikkerhetsmyndighet (NSM) er statens forebyggende sikkerhetsorgan. I følge Lov om forebyggende sikkerhetstjeneste (2001), skal NSM koordinere de forebyggende sikkerhetstiltakene og kontrollere sikkerhetstilstanden. For å gjennomføre dette pålegger Sikkerhetsloven NSM å utføre en rekke tjenester for de virksomheter som er underlagt loven. Altså er det Sikkerhetsloven som er styrende for NSMs virksomhet i Norge. NSM tolker Sikkerhetsloven og lager med bakgrunn i den, forskrifter og veiledninger som er styrende for virksomheter underlagt Sikkerhetsloven.

Evaluerings- og sertifiseringsnemnder

I følge Infosec Assurance and Certification Services (IACS, 2005) er datasikkerhetsevaluering en detaljert eksaminasjon og testing av sikkerhetstrekkene til et IT-system eller et IT-produkt. Dette for å sikre at produktet eller systemet fungerer korrekt og effektiv, samt at det ikke viser noen svakheter (IACS, 2005). Det er sikkerhetsmålet som bestemmer omfanget av evalueringen. Sikkerhetsmålet inkluderer et kravs tillitsnivå som bestemmer hvor streng evalueringen skal være (IACS, 2005). Videre fins det kriterier som standardiserer testene og angir hvilket nivå et system kan ha.

Siden tidlig på åttitallet har det kommet kriterier for klassifisering av systemer. De første kriteriene kom i 1983 og ble publisert av US Department of Defense. Kriteriene het The Trusted Computer Security Evaluation Criteria (TCSEC, 1985), som kanskje er mer kjent som the Orange Book. TCSEC lar systemer bli evaluert i forhold til ulike nivåer, der A1 er det høyeste, deretter B3, B2, B1, så C3-C1 og til sist D. TCSEC ble førende kriterier for sikkerhetsansvarlige i en mengde land i sin tid, men ble endelig pensjonert i 2000. I kjølvannet av at USA laget egne kriterier, kom Storbritannia, Tyskland, Frankrike og Nederland med en felles samling kriterier, der de hadde samkjørt de ulike nasjonale kriteriene. Denne ble kalt Information Technology Security Evaluation Criteria (ITSEC). ITSEC har som TCSEC ulike nivåer, men i ITSEC (1991) brukes nivåene E1 til E6, der E6 er høyeste nivå.

ITSEC (1991) ble etter hvert tatt opp av EU-kommisjonen, og den siste utgaven ble utgitt i juni 1991. Kriteriene som er styrende for dagens systemer er Common Criteria for Information Technology Security Evaluation (CCITSE), også bare kalt Common Criteria (CC).

5.1.2 Metode

Gjennom vår kontaktperson i Program Golf, ble vi satt i kontakt med sikkerhetspersonell i Forsvaret. Med hjelp fra disse fikk vi rede på hvilke lover og regler Forsvaret må forholde seg til, samt hvem som er lovgivende myndighet i forhold til regelverkene. Det viste seg noe vanskelig å finne frem i dokumentene på egenhånd, og vi fikk derfor hjelp til å finne frem til de vesentligste kapitler og paragrafer i regelverkene. Noe av materiellet er graderte dokumenter, blant annet noen lover og forskrifter fra NATO. Disse har vi ikke behandlet spesifikt i oppgaven. Etter å ha fått en oversikt over gjeldende lover og regler, gikk vi nøye igjennom informasjonen og systematiserte sikkerhetskravene.

Gjennom intervjuer med ansatte innen sikkerhet og IKT, fikk vi redegjort for ulike syn på gjeldende sikkerhetskrav sett i forhold til MLS. Dette dreide seg blant annet om hvorvidt gjeldende sikkerhetskrav hindrer Forsvaret i å innføre MLS og hvilke krav som er til størst hinder for dette.

Utover dette har vi hatt personlig kontakt via e-post med Simon Wiseman og Kay Hughes fra QinetiQ, et anerkjent britisk firma innen datateknologi.

Basert på gjeldende sikkerhetskrav og resultater fra intervjuene, vurderte vi hvilke krav som er vanskelige og lette å innfri i forhold til MLS.

5.1.3 Sikkerhetskrav i gjeldende lovverk

Sikkerhetsmessige utfordringer

Et NbF gir store sikkerhetsmessige utfordringer. Ulike tjenester og mekanismer for sikkerhet vil være viktige elementer i fremtidige informasjonsnettverk, og en forutsetning for samvirke mellom systemer og nasjoner. Pedersen et. al. (2004) skriver at for å ivareta sikkerheten må fremtidens nettverk inneholde en rekke sikkerhetsmekanismer, som sikrer konfidensialitet og integritet for informasjon som flyter i nettverket, samt sikring mot at uautoriserte brukere og utstyr ikke får tilgang til nettverket. Sikkerhetsmekanismer må sikre informasjonen på alle lag og innenfor alle tjenester i nettverket. Med informasjon menes: ”*Enhver form for opplysninger i materiell eller imateriell form*”(Sikkerhetsloven, 2001, kap.1, § 3). Sikkerhetsmekanismene må være anerkjent av Forsvarets eksterne partnere og kunne benyttes for sikring av informasjonsutveksling med partnernes systemer. Videre må de være dimensjonert i forhold til resten av Forsvarets informasjonssystem og ikke begrense ytelsen eller funksjonaliteten i tjenestene i vesentlig grad.

Krav til informasjonssikkerhet

De overordnede kravene til informasjonssikkerhet er nedfelt i NATOs bestemmelser, samt i Sikkerhetsloven med tilhørende forskrifter og veiledninger. ”*Forsvarsdepartementet har det overordnede ansvar for forebyggende sikkerhetstjeneste*” (Sikkerhetsloven, 2001, kap.2, § 4). Når det gjelder hvilke krav som legges til grunn ved sikkerhetsgodkjenning av graderte systemer, så er dette relativt omfattende. Sikkerhetsloven omfatter flere fagområder innen sikkerhet; informasjonssikkerhet, objektsikkerhet, personellsikkerhet, og sikkerhetsgraderte anskaffelser. Innen fagområdet informasjonssikkerhet, finnes grunnleggende sikkerhetskrav for informasjonssystemsikkerhet. Selv om informasjonssystemsikkerhet kan sies å være det kapitlet som skal gi de grunnleggende kravene for hvordan man skal sikre et informasjonssystem innenfor en gitt operasjonsmåte og graderingsnivå, gir Sikkerhetsloven som helhet lovmessige krav som også må legges til grunn.

”*Departementets utøvende funksjoner ivaretas av Nasjonal sikkerhetsmyndighet (NSM)*” (Sikkerhetsloven, 2001, kap.2, § 4). Det er ikke alltid mulig å finne konkrete krav til hvordan sikkerheten i et informasjonssystem skal ivaretas. NSM har derfor utarbeidet systemtekniske veiledninger som gir retningslinjer for hvordan man i praksis skal oppnå tilstrekkelig sikkerhet i henhold til loven. ”*NSM er også utøvende organ i forholdet til andre land og internasjonale organisasjoner*” (Sikkerhetsloven, 2001, kap.3, § 8). Og ”*Enhver virksomhet plikter å utøve forebyggende sikkerhetstjeneste i henhold til bestemmelsene gitt i eller i medhold av Sikkerhetsloven*.” (Sikkerhetsloven, 2001, kap.2, § 5).

Krav som er enkle å innfri

Flere av kravene i Sikkerhetsloven (2001) med forskrifter og veiledninger er uproblematiske å innfri. Dette gjelder i første omgang konfidensialitet, integritet og tilgjengelighet. De grunnleggende kravene står oppført i Forskrift om informasjonssystemsikkerhet (2001).

”*Sikkerhetsgradert informasjon skal sikres mot endring og mot at falsk informasjon kan innføres under overføring*” (Forskrift om informasjonssystemsikkerhet, 2002, § 5-5).

Konfidensialitet

Data må beskyttes mot uautorisert tilgang. Kryptering på nettlaget må gi konfidensialitetssikring av gradert informasjon som sendes over kommunikasjonslinjer utenfor beskyttet område, og som er tilpasset grensesnitt og nettjenester for det tjenesteintegrerte nettet i NbF. I følge Pedersen et al. (2004) må ulike typer krypteringsutstyr, både for faste og mobile nett være interoperable, og bør ha felles ledelse og nøkkeladministrasjon. Videre må det etableres løsninger og prosedyrer for samtrafikk med allierte.

Integritet

Data må beskyttes mot uautorisert endring. I NbF må tilgangskontroll være basert på informasjonens gradering, brukernes klarering og autorisasjon gjennom utstrakt bruk av sikkerhetssertifikater og digitale signaturer. I henhold til Pedersen et al. (2004) må informasjonsintegritet sikres ved at informasjonen merkes med graderingsnivå, tidspunkt, kilde og nøyaktighet. Dette vil samtidig gi mulighet for kvalitetsfokus og gi beslutningstaker mulighet til prioritering av sensorer og det informasjonsgrunnlaget som legges til grunn for viktige beslutninger.

Tilgjengelighet

Informasjonsinfrastrukturen må kunne motstå overbelastninger, feil og ødeleggelser. Dette omtales gjerne som robusthet. I følge Pedersen et al. (2004) kan det benyttes redundant lagring av informasjon for å oppnå akseptabel informasjonstilgjengelighet. Redundant lagring innebærer at informasjonen distribueres slik at det finnes flere informasjonsnoder som har lagret samme informasjon. I de tilfeller hvor kommunikasjonsnettene degraderes og ikke klarer å opprettholde nødvendig båndbredde, vil prioritetsmekanismer måtte benyttes. Applikasjonene og informasjons- og databehandlingsnodene i informasjonsnettet må kunne angi prioritet på det som skal overføres, og avvikle trafikken slik at høyest prioritert trafikk ikke forhindres av lavere prioritert trafikk. ”*Å opprettholde informasjonsoverlegenhet og -tilgjengelighet, uansett situasjon, krever store ressurser*” (Pedersen et al. 2004).

Krav som byr på utfordringer

Flyt av data mellom graderingsdomener

Sikkerhetsloven og NATOs sikkerhetsbestemmelser setter grenser for, og stiller krav til sammenkoblinger av systemer med forskjellige graderingsnivåer.

”Hvert sammenkoblet system skal ha en beskyttelse mot andre informasjonssystemer, og sikkerheten i det enkelte system skal bare baseres på mekanismer i vedkommende system” (Forskrift om informasjonssikkerhet, 2001, § 5-4).

Disse mekanismene skal i henhold til Sikkerhetsloven (2001) godkjennes av NSM, og vil i hovedsak være sertifiserte løsninger. Det er bare NSM som kan godkjenne sammenkoblinger av informasjonssystemer med ulikt graderingsnivå. I følge Hvalby (personlig kommunikasjon, 21. januar 2005), henviser NSM i den forbindelse til NATO PRIMARY INFOSEC DIRECTIVE. Dette er et gradert dokument, som etter deres tolkning, ikke tillater sammenkobling av informasjonssystemer fra ugradert til HEMMELIG. NSM har derfor ikke godkjent noen mekanismer for dette eller utarbeidet noen veiledning for hvordan dette skal kunne oppnås. I følge Hvalby (personlig kommunikasjon, 21. januar 2005) er det imidlertid

signaler fra NATO som indikerer at dette endres, noe som også er en forutsetning for et NbF.

I henhold til Sikkerhetsloven (2001) skal informasjon som må beskyttes av sikkerhetsmessige grunner, ha en av følgende sikkerhetsgrader: STRENGT HEMMELIG (eventuelt COSMIC TOP SECRET), HEMMELIG (eventuelt NATO SECRET), KONFIDENSIELT (eventuelt NATO CONFIDENTIAL) eller BEGRENSET. Gjeldende sikkerhetsregime tillater sammenkobling og toveis dataflyt mellom BEGRENSET og ugradert informasjonsdomene, samt automatisk overføring av data fra lavere til høyere graderingsdomene via en diodeløsning. Gjeldende sikkerhetsregime tillater ikke sammenkobling og toveis dataflyt mellom ugradert eller BEGRENSET domene, og HEMMELIG domene.

Høyere gradert informasjon kan ikke behandles på fellesnivå BEGRENSET. Dersom slik informasjon skal håndteres i FIF, må informasjonseier vurdere beskyttelsesbehovet opp mot informasjonsbehovet og eventuelt nedgradere informasjonen. Alternativet er å håndtere slik informasjon i systemer som er godkjent for bruk i et høyere gradert domene.

Evaluering og sertifisering

Kriteriene som er styrende for dagens MLS-systemer er CCITSE, også bare kalt Common Criteria (CC). CC (2003) representerer utfallet av et samarbeid mellom Europa og Nord-Amerika om å lage felles kriterier. CC-prosjektet sammenkobler ITSEC, Canadian Criteria (CTCPEC) og US Federal Criteria (FC) inn i CC. CC (2003) opererer med nivåene Evaluation Assurance Level 1- Evaluation Assurance Level 7 (EAL1 - EAL7), der EAL7 er det høyeste nivået.

"The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a Target of Evaluation (TOE) at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE."(CC, 2003, part 3, s. 53).

- EAL1 - Funksjonelt testet. Dette nivået gir en grunnleggende tiltro, gjennom en analyse av sikkerhetsfunksjonene.
- EAL2 - Bygningsmessig testet. Dette nivået gir en meningsfull økning i tiltro i forhold til EAL1, ved at den krever utviklingstester, sårbarhetsanalyser, og selvstendig testing basert på detaljer gitt i CC.
- EAL3 – Metodisk testet og sjekket. Dette nivået representerer en meningsfull økning i tiltro i forhold til EAL2, ved at den krever mer fullstendig testing av sikkerhetsfunksjonene og mekanismene.
- EAL4 – Metodisk designet, testet og gjennomgått. Dette nivået representerer en meningsfull økning i tiltro i forhold til EAL3, ved at den krever mer design

beskrivelser, mer beskrivelse av implementeringsprosessen og forbedrede mekanismer.

- EAL5 – Delvis formelt designet og testet. Dette nivået representerer en meningsfull økning i tiltro i forhold til EAL4, ved at den krever en delvis formell design beskrivelse. Videre krever den en beskrivelse av hele implementeringsprosessen, en mer strukturert arkitektur, analyser av skjulte kanaler og forbedrede mekanismer.
- EAL6 – Delvis formelt designet og testet. Dette nivået representerer en meningsfull økning i tiltro i forhold til EAL5, ved at den krever en mer omfattende analyse, strukturert representasjon av implementeringen, en mer arkitekturisk struktur, en mer omfattende selvstendig sårbarhets-testanalyse, en systematisk identifisering av skjulte kanaler og en forbedret konfigurasjonsforvaltning.
- EAL7 – Formelt verifisert design og testet. Dette nivået representerer en meningsfull økning i tiltro i forhold til EAL6. Den krever mer omfattende analyse, ved at den bruker formelle representasjoner og en formell overensstemmelse, samt mer omfattende testing.

5.1.4 Synspunkter vedrørende gjeldende sikkerhetskrav

Gjeldende sikkerhetsbestemmelser

Tre av fire intervjuobjekter mente at gjeldende sikkerhetsbestemmelser er helt eller delvis avgjørende for at MLS ikke kan taes i bruk på nåværende tidspunkt. Liberg ga uttrykk for at det er de formelle kravene fra NSM som er for strenge. Per i dag er det ikke lov å sammenkoble systemer, og det er da umulig for IBM som leverandør å diskutere mulige løsninger.

Nakstad påpekte at systemene ikke er klare og at teknologien er for dårlig per i dag. Det er dog liten vits i å utvikle teknologien videre før regelverket åpner for en MLS-løsning. Foreløpig er regelverket åpnet for to nivåer.

Nyquist mente at det er kravene til tiltro som hindrer Forsvaret i å ta i bruk MLS. Han ser vanskeligheter med å gjennomføre fullstendige MLS-løsninger med det tillitsnivået som kreves i dag, men ser muligheter for mer delvise MLS-løsninger.

Wiseman (personlig kommunikasjon, Wiseman, 29. april 2005) fra QinetiQ, mente på sin side at CC-evalueringen ikke bidrar noe særlig til sikkerhet. Videre uttrykte han at CC-evalueringen ikke fokuserer på de riktige tingene. ”*CC does not focus on what really matters, cannot reason about separation, cannot reason about content checking and is horribly expensive and overburdened with bureacracy.*” (Personlig kommunikasjon, Wiseman, 29. april 2005). I tillegg har Wiseman sammen med Pomeroy, skrevet at “S*ystem designs requiring more than Common Criteria EAL4 assurance should be avoided, because higher assurance is only found in a few specialised products.”* (Pomeroy & Wiseman, 1998, s. 3).

Avgjørende sikkerhetskrav vedrørende MLS

Vedrørende hvilke av gjeldende sikkerhetskrav som er mest avgjørende, viste Liberg til Sikkerhetsloven med forskrifter og veiledninger.

Nakstad på sin side mente at NATOs Infosec nummer 33 er mest avgjørende. Dette dokumentet er gradert, og vi har derfor ikke behandlet dette spesifikt i oppgaven.

Nyquist påpekte at evaluerings- og sertifiseringskravene er altfor høye. Kravet er ofte at alle underliggende mekanismer er sertifiserte sammen med et eventuelt system.

Hvinden anså kravet til tiltro som det tøffeste kravet innen MLS. Det dreier seg da om tiltro til at softwaren er god nok. Videre nevnte han Sikkerhetsloven (2001) som forbyr hemmelige systemer å kobles mot Internett, samt NATO-policyen. Sistnevnte er noe myket opp i forhold til tidligere, da det nå er åpnet for enveisløsninger med informasjonsflyt nedenfra og opp, med høy tiltro. Han påpekte imidlertid at det er viktig å få informasjonsflyt ovenfra og ned, siden beslutninger ofte taes høyt oppe og må ut igjen til personer via lavere gradert nivå. Det er riktignok mest informasjon som går nedenfra og opp, som for eksempel værdata og antivirusfiler fra Internett. Utfordringen ligger i at noe av informasjonen går ovenfra og ned.

Endring av kravene

Både Nakstad og Liberg mente at det er helt nødvendig å endre gjeldende sikkerhetskrav for å gjøre det mulig å implementere MLS i Forsvaret. MLS innebærer å knytte flere systemer sammen, og dette er umulig med dagens sikkerhetskrav.

Nakstad påpekte at dette vil gjøre Forsvaret mindre sikkert. Slik det er i dag er det umulig å angripe HEMMELIG fra ugradert.

Liberg snakket om en gråsone vedrørende sikkerheten. Per definisjon vil sikkerheten bli dårligere, men ikke så avgjørende at hele løsningen settes på spill. En senkning av gjeldende krav vil åpne mulighetene for å innføre MLS, og det vil gjøre det mulig å diskutere hvilke systemer som fyller de nye kravene. Liberg mente at hvis Forsvaret senker kravene kan blant annet systemene fra IBM vurderes, og planene om et NbF kan realiseres. Han sa videre at NSM erfaringsmessig er ute etter det beste og vil at alle mulige krav skal tilfredsstilles, noe som hindrer implementering av gode og rimelige løsninger.

Hvinden mente at det å endre sikkerhetskravene så mye at det kan åpnes for MLS er svært urealistisk. Videre sa han at en eventuell senkning av dagens sikkerhetskrav vil føre til større fare for kompromittering av data, dårligere sikkerhet, samt akseptproblemer. Tiltroen til MLS-produktene er ikke gode nok til å møte HEMMELIG/BEGRENSET.

Nyquist på sin side, mente at man i stedet for å fokusere utelukkende på MLS, burde dreie diskusjon og utvikling mer mot oppnåelige løsninger basert på risikovurderinger, der fokus rettes mot konklusjonene for hva som er nødvendig og tilstrekkelig. Dersom dette resulterer i at man på enkelte funksjonelle elementer må ha stor grad av tillitt, så kan det aksepteres.

Arbeid med sikkerhetsbestemmelsene

Det er ingen som jobber med å endre sikkerhetskravene, for på denne måten å åpne for MLS i Forsvaret. Det er NSM som stiller kravene i Norge, og de må følge NATO i henhold til internasjonale sikkerhetsbestemmelser. Dette henger nøye sammen med høygradert nasjonalt nivå da dette ofte er koblet mot NATO. NSM trenger ikke følge NATO-bestemmelsene for nasjonalt graderte systemer så lenge disse ikke er koblet opp mot NATO.

Arbeidsgrupper i NATO C3-board, Subcommitees 4, ser på sammenkoblinger av systemer. Her har NSM en representant. Landene kommer sammen og setter reglene, og i følge Hvinden er det de som er mest forsiktige med tanke på sikkerhet, som oftest får viljen sin. Holdningene er forskjellige fra land til land, og det er de strengeste som styrer. Det som vedtas nedfelles i formelle dokumenter.

Hvinden sa at det for ikke lenge siden kom en NATO-policy som åpnet for bruk av diode med enveis overføring. Tidligere var det absolutt ikke lov å sammenkoble systemer mot Internett. NSM er i likhet med representanter fra alle andre nasjoner, forpliktet til å signere et dokument som heter CM-5515. Dette dreier seg om informasjonssikkerhet, fysisk sikkerhet og dokumentsikkerhet.

5.1.5 Oppsummering

Sikkerhetsloven og NATOs sikkerhetsbestemmelser setter grenser for, og stiller krav til sammenkoblinger av systemer med forskjellige graderingsnivåer. Det er dette som er den største utfordringen i gjeldende sikkerhetsbestemmelser, i forhold til innføring av MLS i Forsvaret.

Sikkerhetsloven stiller krav om at hvert sammenkoblet system skal ha en beskyttelse mot andre informasjonssystemer, og at sikkerheten i det enkelte system skal bare baseres på mekanismer i vedkommende system. Enhver sammenkobling av informasjonssystemer med ulikt graderingsnivå, må godkjennes av NSM. De viser til NATO PRIMARY INFOSEC DIRECTIVE, som ikke tillater sammenkobling av informasjonssystemer fra ugradert til hemmelig.

Flesteparten av intervjuobjektene mente at det er gjeldende sikkerhetsbestemmelser som hindrer Forsvaret i å innføre MLS i dag; først og fremst fordi lovverket, som nevnt tidligere, ikke tillater sammenkobling av informasjonssystemer med ulike graderingsnivåer.

Videre må MLS-systemer tilfredsstille evaluerings- og sertifiseringskrav i CC. Flere mener at disse kravene er for høye, og altfor vanskelige å innfri.

Det er ingen som jobber med å endre kravene i sikkerhetsbestemmelsene. Flere av intervjuobjektene mente faktisk at det er umulig å innføre et fullverdig MLS-system i Forsvaret, hvis ikke gjeldende sikkerhetskrav senkes.

5.2 Delproblem 2: Kartlegging av Multilevel Security

Vi skal redegjøre for teorier og strategier innen MLS, samt presentere realiserte MLS-systemer.

5.2.1 En kort historisk oversikt

Det har siden sent på sekstitallet blitt utviklet datasikkerhetsmodeller. En av de første modellene var High Water Mark modellen, som ble utviklet av Weissman (1969). Systemet som modellen skulle implementeres i var et av de første systemene som prøvde å implementere en softwarekontroll for gradert informasjon. I 1971 kom Lampson med en modell som ble kalt for tilgangsmatrisemodellen. Modellen var ikke primært laget for forsvarsstrukturer, da den var mer som en abstraksjon av et operativsystem. Modellen ble mye brukt fordi den tillot flere implementeringsteknikker og den var en svært enkel og generell i bruk. UCLA-kjernen (Farber & Popek, 1978; Kemmener, Popek & Walker, 1979) og MULTICS (Saltzer, 1974; Schroeder, 1975; Clark, Saltzer & Schroeder, 1977; Ames et al., 1975*)* er eksempler på systemer som tilgangsmatrisen ble brukt i. I 1973 presenterte Lampson en annen modell.

I 1973 kom BLP-modellen, som ble en foregangsmodell for fremtidige modeller. Det har blitt utgitt mange ulike reviderte versjoner av BLP-modellen, blant andre Biba-modellen (Biba, 1977), Dennings (1976) informasjonsflytmodell og modellen til Feiertag, Levitt og Robinson (1977).

Det har med årene også kommet noen datasikkerhetsmodeller som ikke har sin bakgrunn i BLP-modellen. Vi kan for eksempel nevne HRU-modellen (Harrison, Ruzzo og Ullman, 1976), Take-grant-modellen (Lipton & Snyder, 1977; Snyder, 1977) og TAM-modellen (Sandhu, 1992). Alle disse modellene er basert på tilgangsmatrisemodellen til Lampson (1971), men ingen av disse er typiske MLS-modeller.

5.2.2 Hva skjedde etter 1990?

Det var tidlig på syttitallet at det virkelig tok av med å utvikle modeller for datasikkerhet. USA med sitt forsvar i spissen, bevilget store summer til utvikling av formelle datasikkerhetsmodeller.

Det var en felles mening innad i utviklingsmiljøet at løsningen på å få et sikkert system, var å konstruere et MLS operativsystem (Macenzie & Pottinger, 1997). BLP-modellen ble som en far for alle andre MLS-modeller. Etter hvert som årene gikk, ble programmeringskostnadene mindre og yteevnen større, samtidig ble datanettverk essensielle for å dele arbeid og ressurser. Det ble bygget lokale nettverk for å dele printere og filer lenge før datamaskiner rutinemessig ble tilknyttet Internett. I forsvarssammenheng måtte flernivås datadeling adresseres i et nettverksmiljø. Til å begynne med gikk forsvarsnasjoner over til nettverk med billige maskiner, for midlertidig å unngå MLS-problemet. I stedet for å ta tak i problemet med datadeling, begynte flere organisasjoner å bruke separate nettverk for å operere på ulike sikkerhetsnivåer, der alle kjørte i fellesnivå operasjonsmåte.

Denne tilnærmingen hjalp ikke stort for etterretningsmiljøene. Det var ikke praktisk mulig å skaffe individuelle nettverk for alle mulige kombinasjoner med felter og kodeord, siden det var alt for mange å håndtere. Dessuten brukte etterretningsanalytikere ofte å kombinere informasjon fra flere felter, for å lage et dokument med en annen gradering. I praksis krevde dette arbeidet et MLS-skrivebord og ofte kommunisering over et MLS-nettverk.

Databruken endret seg altså fra flerbrukersystemer til nettverkssystemer. Dette hadde ikke BLP-modellen tatt høyde for, og den ble derfor ikke lenger en veiledende sikkerhetsmodell. Det oppstod et behov for en modell som kunne ta høyde for integrasjon mellom datamaskiner, med andre ord kommunikasjon i ett nettverk. Nesten samtidig som behovet for en ny type modell kom, sluttet den kalde krigen. Dette førte til at USA kuttet i forsvarsbudsjettet, hvilket medførte at det ikke ble utviklet noen ny klassisk modell som kunne ta over for BLP-modellen fra det amerikanske forsvaret. Den kommersialiserte siden av datasikkerhet hadde ikke noe sterkt behov for å verifisere et system så høyt som det Forsvaret trengte, og derfor uteble utviklingen av formelle modeller. Følgelig har det kommet svært lite MLS-modeller etter 1990. Europa og NATO har senere involvert seg mer i utviklingen av MLS-systemer, men det er lite publisert informasjon rundt dette.

5.2.3 Metode

Vi brukte kvantitativ metode i form av litteraturinnsamling, for å besvare dette delproblemet. For å finne informasjon om de ulike teknologiene, søkte vi først og fremst i litteraturdatabaser, deriblant IEEE, ISI, EBSCO og Springer og på Internett. I tillegg var vi innom biblioteket på høgskolen og lånte diverse bøker om datasikkerhet. Vi fant svært mye informasjon om emnet, og brukte mye tid på å gå igjennom og systematisere stoffet. Mye av informasjonen var basert på sekundærdata. I utvelgelsen av den informasjonen vi skulle bruke i det videre arbeidet, la vi vekt på at denne fortrinnsvis inneholdt primærdata. Vi planla videre å bruke resultatene fra intervjurunde en i besvarelsen. Intervjuobjektene hadde imidlertid liten kunnskap vedrørende modeller, arkitekturer og strategier med fullverdig MLS-funksjon. De fleste kjente til Bell-LaPadula som ligger til grunn for Orange book modellen (Trusted Computing Base). Ellers snakket de mye om andre løsninger med delvis eller ingen MLS-

funksjon. Vi fikk altså ingen gode ideer om hvilke modeller vi burde fokusere på ut fra intervjuene.

På grunn av den store datamengden satte vi opp noen kriterier for å avgjøre hvilke teorier og strategier vi skulle presentere i rapporten. Vi ønsket å lage et utvalg som representerte den historiske utviklingen, forskjellige MLS-tankeganger og nåværende situasjon innen MLS. I tillegg la vi vekt på å plukke ut anerkjente teorier og strategier, og vurderte dette ut ifra hvor hyppig modellene, metodene og strategiene er referert i artikler og bøker. Vi endte opp med et utvalg bestående av seks formelle modeller, en strategi og en metode.

Teoriene og strategien som vi har presentert i rapporten, er hovedsakelig basert på fagartikler funnet i litteraturdatabaser, men noe er som sagt også hentet fra bøker og Internett. Videre er noe av teorien supplert med uttalelser fra fagpersoner, blant annet fra QinetiQ, et anerkjent britisk firma innen datateknologi.

Det har blitt laget utallige modeller med ulike egenskaper opp igjennom årene. Vi har valgt å presentere et historisk snitt som spenner seg fra den første MLS-modellen fra 1973 til en aktuell metodisk prosess fra 2001. Vi ønsker med vårt modellutvalg å få belyst de ulike egenskapene som verserer i MLS-modeller. Det viste seg at det er laget utallige modeller, strategier og metoder for MLS. Utfordringen ble da å plukke ut de beste og mest betydningsfulle modellene. Samtidig ville vi ha et utvalg som representerte forskjellige oppbygningsmetoder og prinsipper innen MLS.

Utover dette har vi kontaktet enkelte ressurspersoner innen MLS. Vi har blant annet fått hjelp og nyttig informasjon fra er R.E. Smith, informasjonssikkerhetsekspert ved University of St.Thomas i Minnesota. Han har blant annet skrevet kapitlet om MLS i en ny lærebok innen sikkerhet. Boken er foreløpig ikke utgitt, men Smiths bidrag er tilgjengelig fra universitetets hjemmesider. Vi har kommunisert med Smith via e-post, og han har vært svært behjelpelig med å svare på spørsmål. Videre har vi fått hjelp og informasjon fra K. J. Hughes ved QinetiQ, som er Englands svar på Forsvarets Forskningsinstitutt. Han har blant annet skrevet mye om Domain Based Security. I tillegg har vi vært i kontakt med S. Wiseman som også er ansatt i QinetiQ. Sistnevnte har bred kunnskap innen Purple Penelope og har gitt oss nyttig informasjon innenfor dette området.

Valg av modeller

Tabell 3: Oversikt over de modellene, strategien og metoden vi har valgt.

Navn	År	Sikkerhetspolitkkmodell	Arbeidsflytmodell	Strategi	Metode
BLP	1973	X			
Rev.BLP	1977	X			
MMS	1984	X			
SNet	1987	X			
Vijay	1990	X	X		
Atluri	1997		X		
NRL	1999			X	
DBSy	2000				X

BLP = Bell & La Padula (1973), BLP rev. = Feiertag et al. (1977), MMS = Landwehr (1984), SNet = Glasgow & MacEwen (1987), Vijay = Varadharajan (1990), Atluri= Atluri et al.(1997), NRL = Kang et al. (1999), DBSy = Robinson (2001); Hughes (2002); Warrener (2003).

Vi har valgt ut BLP-modellen (Bell & La Padula, 1973), siden dette er den klassiske modellen som de fleste senere modeller har bygget videre på. Deretter har vi valgt Feiertag et. al.(1977), som er den mest brukte revideringen av BLP-modellen (1973). Den militære meldingsmodellen til Landwehr, Heitmeyer og Mclean (1984) har vi også tatt med, siden den representerer en annen tilnærming til BLP-modellen (1973). Den militære meldingsmodellen er dessuten svært lik meldingstjenesten i det norske forsvarets personlige brukersystem (PBS) i oppbyggingen, noe som også gjorde sitt til at vi valgte denne. Videre har vi tatt med en modell som er laget for et konkret system, nemlig SNet-modellen til Glasgow og MacEwen (1987). Denne har vi tatt med for å vise at det går an å skreddersy en modell til et spesielt system. Glasgow og MacEwens (1987) modell er for øvrig lett å forstå, da presentasjon av modellen er svært enkel.

Siden det har kommet svært få formelle tilgangsmodeller etter nittitallet, har vi valgt å ta med noen formelle MLS-arbeidsflytmodeller. Disse belyser problemstillingen til Forsvaret i form av at de trenger å utføre oppgaver i forskjellige nivåer, uten at det går på bekostning av sikkerheten. Minuset med en ren arbeidsflytmodell er at den ikke tar for seg tilgangssikkerhet. Den første arbeidsflytmodellen vi har valgt, er tilgangs- og flytmodellen til Vijay Varadharajan (1990). Dette er den nyeste formelle MLS-modellen vi har kommet over med tilgangssikkerhet. Den andre arbeidsflytmodellen vi har tatt med, er Atluri, Huang og Bertinos (1997) sikre MLS-arbeidsflytmodell. Begge disse modellene presenterer hvordan en sensitiv arbeidsflyt går fra et nivå til et annet. Vi har også tatt med Kang, Froscher, Eppinger og Moskowitzs (1999) strategi for implementering av en militær arbeidsflyt. De kommer med et praktisk eksempel for hvordan en kan få til en MLS-arbeidsflyt i et militært nett. Den siste modellen vi har tatt med er en metodisk prosess for å bygge et MLS-system. Domenebasert sikkerhet (Robinson, 2001; Hughes, 2002; Warrener, 2003) er en metode som er utviklet av det britiske forsvaret og Defence Evaluation And Research Agency (DERA) på slutten av nittitallet.

Valg av MLS-systemer

Tabell 4: Oversikt over valgte MLS–systemer.

Navn	Operativsystem	Meldingstjeneste	Fullverdig MLS	Delvis MLS	Annet
IBM - Fujifilm Medical Systems			X		
Sun Trusted Solaris v1.1	X				
Personlig Brukersystem		X			
Partisjonert fellesnivå				X	
SyBard					X
RAF's LITS			X		
AT&T's System V/MLS	X				
CMW					X

Vi har her valgt å presentere de systemene som intervjuobjektene nevnte i intervjuene, dette gjelder IBMs farmasiløsning, Sun Trusted Solaris, Personlig Brukersystem (PBS) og Partisjonert fellesnivå. Videre har vi valgt å ta med noen av de realiserte systemene vi har kommet over i litteratursøk. Dette gjelder systemene SyBard, The Royal Air Force's Logistics Information Technology System (RAFs LITS), American Telephone and Telegraph Company's (AT&T) System V/MLS og Compared mode workstations (CMWer).

Rammeverk for sammenlikningen

Modellene, strategien og metoden

Vi har laget rammeverket der vi sammenlikner modellene, strategien og metoden. Selv om strategien og metoden strengt tatt ikke kan sammenliknes med de formelle modellene, så gjør vi dette for lettere å se egenskapene og hensikten med dem.

Vi har valgt å sammenlikne modellene med hensyn til hvilken motivasjon de er blitt laget på, hvilket syn på sikkerhet som er lagt til grunn, samt andre faktorer som belyser modellenes egenskaper.

Motivasjonen sier noe om bakgrunnen for utviklingen av modellen, strategien og metoden. Er den laget for et spesielt system? Eller er den laget på et generelt grunnlag, slik at den kan brukes som veiledning for fremtidige konstruksjoner?

Synet på sikkerheten sier noe om hva modellen, strategien eller metoden baserer sin sikkerhet på. Det er per i dag to forskjellige hovedsynspunkter. Det første er modellering av tilgang med hensyn til objekter, og det andre er modellering med hensyn til informasjonsflyt mellom objektene.

Vi har også tatt med egenskaper som om det har blitt implementert systemer basert på modellen, om modellen er formell, og om modellen primært er laget for forsvarsbruk.

MLS-systemene

Vi har laget et rammeverk der vi sammenlikner de ulike realiserte systemene med hverandre, der vi har valgt å sammenlikne systemene med hensyn til om systemet er i bruk i dag, om systemet er et fullverdig MLS system, og eventuelt hvilken tiltro systemet har fått i en evaluering.

5.2.4 Bell-Lapadula-modellen

Introduksjon og motivasjon

Det amerikanske luftforsvaret sponset konstruksjonen av noen formelle datasikkerhetsmodeller som en del av et datasikkerhetsprogram. Forskningen innen de formelle modellene ble blant annet utført på MITRE av Bell og La Padula (1973) og på Case Western Reserve University av Walter et al. (1974). De utviklet hver sin modell. Den mest kjente av dem er modellen til Bell og La Padula. BLP-modellen er i dag den mest anerkjente tilnærmingen til MLS. Modellen fanger effektivt inn de viktigste aksessrestriksjonene implisert av tradisjonelle militære sikkerhetsnivåer.

”*Most MLS mechanisms implement Bell-LaPadula or a close variant of it. Although Bell-LaPadula has accurately defined a MLS capability that keeps data safe, it has not led to the widespread development of successful multilevel systems. In practice, developers have not been able to produce MLS mechanisms that work reliably with high confidence, and some important defense applications require a "write down" capability that renders Bell-LaPadula irrelevant.*” (Smith, 2005).

Syn på sikkerhet

I BLP-modellen (Bell & La Padula, 1973 & 1976) er det modellering av tilgang til objektene som gjelder. Subjekter prøver å overføre informasjon til objektene i datasystemet. Subjekter kan for eksempel være programmer og prosesser, mens objekter kan være filer, innretninger for input eller output og meldinger. Alle subjekter og objekter bærer en etikett med gjeldende sikkerhetsnivå, som er subjektets klareringsnivå eller objektets graderingsnivå.

I BLP-modellen (Bell & La Padula, 1976) er det to ting en tilgang kan gjøre på objekter. Den ene er å kunne lese objektet, og den andre er å kunne endre objektet. Det blir da fire måter et subjekt kan få tilgang til et objekt på, og de fire tilgangsmetodene er:

- Lese: Subjektet kan lese objektet, men ikke modifisere det.
- Skrive: Subjektet kan skrive objektet, men det kan ikke lese det.
- Kjøre: Subjektet kan kjøre objektet, men det kan ikke lese eller skrive til objektet direkte.

- Lese/skrive: Subjektet kan både lese og skrive objektet.

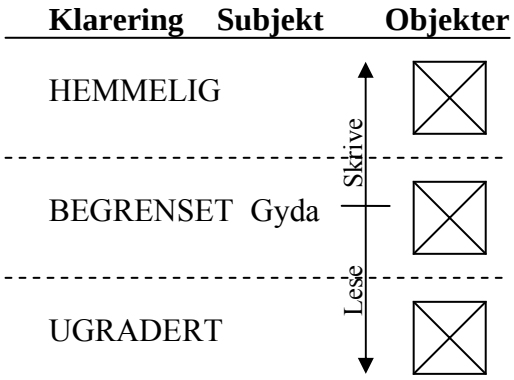
I tillegg defineres et tilgangsattributt, som er likt et eierflagg. Attributtet lar et subjekt få muligheten til å sende over alle eller noen av tilgangsmetodene det har for et objekt til et annet subjekt.

Det som gjør BLP-modellen (Bell & La Padula, 1976) til en MLS-modell er to enkle regler som fremtvinger tilgangsrestriksjoner: den enkle sikkerhetsegenskapen og stjerneegenskapen.

- Den enkle sikkerhetsegenskapen: Det er ikke lov til å lese opp i nivåene. Et subjekt har lov til å lese et objekt bare hvis subjektets sikkerhetsklarering dominerer sikkerhetsnivået til objektet, det vil si hvis subjektet har en høyere sikkerhetsklarering enn objektet.
- Stjerneegenskapen: Det er ikke lov til å skrive ned i nivåene. Det vil si at et subjekt bare har lov til å skrive et objekt dersom dets sikkerhetsklarering dominerer objektets klarering. Altså kan ikke et høyere nivås subjekt skrive til et lavere nivås objekt.

Smith (2005) har oppsummert egenskapene til disse to på følgende måte:
*"The simple security property is obvious: it prevents people (or their processes) from reading data whose classification exceeds their security clearances. Users can't "read up" relative to their security clearances. They can "read down," which means that they can read data classified at or below the same level as their clearances. The *-property prevents people with higher clearances from passing highly classified data to users who don't share the appropriate clearance, either accidentally or intentionally. User programs can't "write down" into files that carry a lower security level than the process they are currently running. This prevents Trojan horse programs from secretly leaking highly classified data."* (Smith, 2005).

Som en oppsummering forebygger disse reglene at KONFIDENSIELL informasjon flyter ut til mindre tillitsfulle subjekter. Figuren nedenfor beskriver dette. Dersom Gyda har sikkerhetsklareringen BEGRENSET, kan hun ikke lese HEMMELIGE objekter og ikke skrive ugraderte objekter.



Figur 9: Et eksempel på tilgangskontroll i BLP-modellen.

I tillegg har Bell og La Padula (1976) laget noen regler for å styre overgangen fra en tilstand til en annen. Disse reglene ble kalt skjønnsmessig sikkerhet, og de ble dannet på grunnlag av den kjente militære reglen need-to-know. Skjønnsmessig sikkerhet lar en person som har tilgang til et dokument, utvide tilgangen til det objektet, slik at et annet individ kan få tilgang til det.

Tanker rundt modellen

Det amerikanske forsvaret la inn store ressurser på å forske innen datasikkerhet, men MLS-mekanismene greide ikke å skaffe den sikkerheten som ble krevd. I følge Smith (2005) var en av grunnene at sikkerhetsforskerne og systemutviklerne fant det komplett umulig å beskytte en informasjonsflyt mellom ulike sikkerhetsnivåer i et MLS-system. Smith (2005) fremhever virustrusselen som et annet problem. Grunnen til dette er at BLP-modellen ikke beskytter nivåene for virusspredning. Dersom et lavere nivå får et virus, så gjøres det ingenting for å stoppe viruset i å komme til et høyere nivå. Problemet ble bevist av Cohen (1984). Han satte inn et virus på et ugradert nivå i et BLP-implementert system. Det viste seg raskt at viruset raskt ble spredd til alle sikkerhetsnivåene i systemet. Grunnen til den raske spredningen av viruset var ikke feil i implementeringen, men det beviste at det var en svakhet i BLP-modellen.

En annen svakhet i BLP-modellen (Bell & La Padula, 1973), er at modellen ikke tillater nedgradering av informasjon. Dette førte til at det ble en stor mengde med overgradert informasjon på systemene, noe som også er et problem i Forsvaret i dag. Ifølge Smith (2005) førte nedgraderingsproblemet til at forsvarsmiljøene mistet interessen for BLP-baserte produkter. BLP modellen hadde også sine sterke sider. Den største styrken til modellen var at den igjennom stjerneegenskapen og den enkle sikkerhetsegenskapen, gjorde det mulig for andre å teste ut ulike teorem. Dette er en av grunnene til at den ansees som den klassiske MLS-modellen. Samtidig gjorde det sitt til at modellen ble mye brukt som grunnlag til andre MLS-modeller.

5.2.5 Revidert Bell-La Padula

Introduksjon og motivasjon

Etter hvert har BLP-modellen (Bell & La Padula, 1973 & 1976) blitt modifisert og revidert av mange, for at den best skal passe til forskjellige design og ulike implementeringsprosjekter. Vi kan blant annet nevne MULTICS-kjernen (Schroeder, Clark & Saltzer, 1977) til det amerikanske luftforsvarets dataservicecenter, Millens (1976) utvidelse, SIGMA-meldingssystemets utvidelse (Ames & Oestreicher, 1978) og sist, men ikke minst, SCOMP (Bonneau, 1980) som er beskrevet i kapittel 2.2.4.

Den mest fyldige og mest brukte reviderte versjonen av BLP-modellen er gitt av Feiertag, Levitt, og Robinson (1977). De presenterte to MLS-modeller, der den første er en

generalisering av BLP-modellen (Bell & La Padula, 1973) og Walter-modellen (Walter et al., 1974). Den andre modellen er en reformulering av den første BLP-modellen, og er svært lik BLP-modellen. Grunnen til forskjellen er at den er enklere å bevise, noe som førte til at BLP-modellen (Bell & La Padula, 1973) ble mer populær. Feiertag et al. beviser videre i artikkelen at disse modellene gir MLS og at de er sikre for en gitt systemstruktur. Reformuleringen av BLP modellen, ble også brukt i etterkant av artikkelen til å automatisere verifikasjonsprosessen til en hel del systemer.

Syn på sikkerhet

Modellen til Feiertag et al. (1977) innlemmer informasjonsflyt i modellen, noe som den opprinnelige modellen til Bell og La Padula ikke gjorde. Altså modellen modellerer flyt av informasjonsflyt mellom objektene og ikke tilgang til objektene som den opprinnelige BLP modellen (1973) til Bell og La Padula gjorde.

I den reformulerte modellen, definerer Feiertag et al. (1977) et flernivåsystem til å være følgende ni elementer; tilstand, initialtilstand, sikkerhetsnivåer, sikkerhetsrelasjoner, synlige funksjonsreferanser, funksjonsreferansenivå, resultater og tolker. Ut fra disse ni elementene definerer Feiertag et al. (1977) et multilevel sikkert system som:
"If two sequences of operations are each applied to a system in the same state and if these sequences differ only in operations whose level is not less than or equal to some level, then any operation of that level that is invoked immediately following the two sequences will return the same result. In other words, the operations whose level is not less than or equal to this level cannot effect results visible to the level." (Feiertag et al., 1977, s. 59).

Tanker rundt modellen

Det har som sagt tidligere kommet flere reformuleringer av BLP modellen, og vi har her nevnt en av de mest brukte reformuleringene. Feiertag et al. (1977) var de første som innlemmet informasjonsflyt i BLP modellen, noe som gjorde sitt til at den ble mye brukt og omtalt. Selv om modellen ble reformulert og fikk et annet syn på sikkerheten, så tok likevel Feiertag et al. (1977) med seg de dårlige egenskapene som vi nevnte i den originale BLP modellen. Modellen til Feiertag et al. (1977) ble da etter hvert, sammen med den originale BLP modellen, sett bort ifra i militære miljøer.

5.2.6 Den Militære Meldingsmodellen

Introduksjon og motivasjon

BLP-modellen (Bell & La Padula, 1973 & 1976) er ifølge Landwehr, Heitmeyer og Mclean (1984) upraktisk når den skal brukes i reelle systemer. I enkelte tilfeller må en bruker kunne anrope operasjoner, noe som kanskje strider imot stjerneegenskapen. For eksempel må en bruker kunne trekke ut et ugradert avsnitt fra et KONFIDENSIELT dokument og bruke det i et ugradert dokument. Dette strider imot stjerneegenskapen, og vil ikke kunne gjøres i et BLP-

basert system. For å unngå dette problemet kom Landwehr et al. (1984) med en annen tilnærming. I stedet for å starte med en applikasjonsuavhengig abstraksjon, for så å prøve å lage en applikasjon på toppen av den, starter de heller med en applikasjon og prøver via den å utlede restriksjonene som systemet må overholde. Videre har de laget en sikkerhetsmodell til militære meldingssystemer, MMS- modellen.

Modellen til Landwehr et al. (1984) tar for seg følgende:

- Brukere og deres ulike roller.
- Objekter som kan inneholde andre objekter.
- De ulike relevante mekanismene som må til for å håndheve sikkerhet.

Landwehr et al. (1984) har definert noen betingelser som skal brukes til å beskrive hvordan en bruker ser på systemets operasjoner. Videre har de tatt med noen sikkerhetsantagelser som styrer meldingssystemets prosesser, og tilslutt har de en formell versjon av modellen. De presenterer også et grunnleggende sikkerhetsteorem.

Modellen til Landwehr et al.(1984) støtter ikke revidering av meldinger, selv om slike meldingssystemer har et klart behov for det. Sikkerhetsmodellen fokuserer på påstander. Hvis disse er korrekt utført, vil påstandene forebygge sikkerhetsbrister. Selve modellen har ingen restriksjoner på hvilke teknikker som kan brukes for å implementere meldingssystemet, heller ikke noen som helst verifiseringsmåte for å sjekke at systemet overholder reglene til modellen. Landwehr et al.(1984) gjør dette for at det skal være enkelt å videreutvikle modellen. De mener at en implementering basert på en formell spesifikasjon og å ha bevist dens riktighet er like godt som at en implementering har sikre kjerner og tiltrodde prosesser.

Syn på sikkerhet

Definisjonene som Landwehr et al.(1984) presenterer samsvarer med generell bruk og er med for å gi en tydelig basis for modellen. Landwehr et al. (1984) skiller mellom objekter som er singelnivå og containere som er multinivå.

Brukerens oppfatning av en MMS-operasjon

Landwehr et al.(1984) viser hvordan en bruker kan få tilgang til et system. Personer kan bare få tilgang til systemet ved å logge inn. For å logge inn må personen skrive inn en bruker-ID, samt et passord eller liknende, som systemet sjekker ut. Ved en suksessfull autentisering, får brukeren tilgang til operasjonene, avhengig av hvilken rolle og tilgang personen har. Ved å bruke operasjonene kan brukeren se på eller modifisere objekter eller containere.

Sikkerhetsantagelser

Det vil alltid være mulig for en gyldig bruker å bringe informasjon som brukeren har tilgang til i fare. For å skape tillit til systemsikkerhet basert på brukerens oppførsel, har Landwehr et al.(1984) laget noen antagelser som bare brukeren kan håndheve:

- A1: Systemsikkerhetsoffiseren gir klareringer, anordningsklareringer, og han lager de ulike rollene.
- A2: Brukeren skriver inn den korrekte klassifiseringen når han lager, redigerer, eller omklassifiserer informasjon.
- A3: Innen en klassifisering adresserer brukeren meldinger og definerer tilgangssett for entiteter, slik at brukere med en gyldig need-to-know kan se informasjonen.
- A4: Brukeren skal med riktighet kontrollere informasjon som er kommet fra containere som er merket med CCR.

Sikkerhetspåstander

Landwehr et al.(1984) laget noen påstander som må overholdes for å få et MLS-meldingssystem:

1. Autorisasjon: En bruker kan bare anrope en operasjon til en entitet, hvis brukerens ID eller brukerens rolle er i entitetens tilgangssett sammen med operasjonen som brukeren i utgangspunktet tilkalte.
2. Klassifiseringshierarki: Klassifiseringen til en container er alltid minst like høy som maksimum til klassifiseringene som entitetene inneholder.
3. Endringer til objekter: Informasjon som er tatt bort fra et objekt, arver klassifiseringen som det gjeldende objektet har. Informasjon som er innsatt i et objekt må ikke ha klassifisering som er høyere enn klassifiseringen til objektet.
4. Visning: En bruker kan bare se en entitet med en klassifisering som er mindre enn, eller lik brukerens klarering og klassifiseringen til output-mediet.
5. Tilgang til CCR-entiteter: En bruker kan bare ha tilgang til en indirekte tilsiktet entitet med en container merket CCR hvis brukerens klarering er større enn, eller lik klassifiseringen til containeren.
6. Oversetting indirekte av referanser: En bruker kan holde ID-en til en entitet han indirekte har referert til, hvis han er autorisert til å se entiteten via den referansen.
7. Merkingskrav: Alle entiteter som er vist av en bruker må være merket med brukerens klassifisering.
8. Setting av klareringer, roller og innretningsnivåer: Bare en bruker som har rollen systemsikkerhetsoffiser kan sette klareringer, roller og innretningsnivåer.
9. Nedgradering: Ingen klassifiseringsmerker kan bli nedgradert. Eneste unntak er hvis en bruker med rolle som nedgraderer, har anropt en nedgraderingsoperasjon.
10. Utløsing: Ingen utkast kan bli utløst. Eneste unntak er hvis en bruker har rolle som utløser. Bruker-IDen til utløseren må være bokført i utløserfeltet til utkastmeldingen.

Tanker rundt modellen

Modellen til Landwehr et al.(1984) er bygget for å representere brukergrensesnittet i et meldingssystem. Etter vår mening er det vanskelig å se hva som er tiltrodd i dette systemet. Systemet vil antageligvis inneholde operativsystem, skjermer, databaser, teksteditorer, ulike formateringsprogrammer og kontrollprogrammer. Det virker som at Landwehr et al. (1984)

antar at systemet er fritt for trojanske hester, noe som er en alt for lett utvei. Landwehr et al.(1984) gir dessuten ikke noen veiledning for hvordan dette skal implementeres.

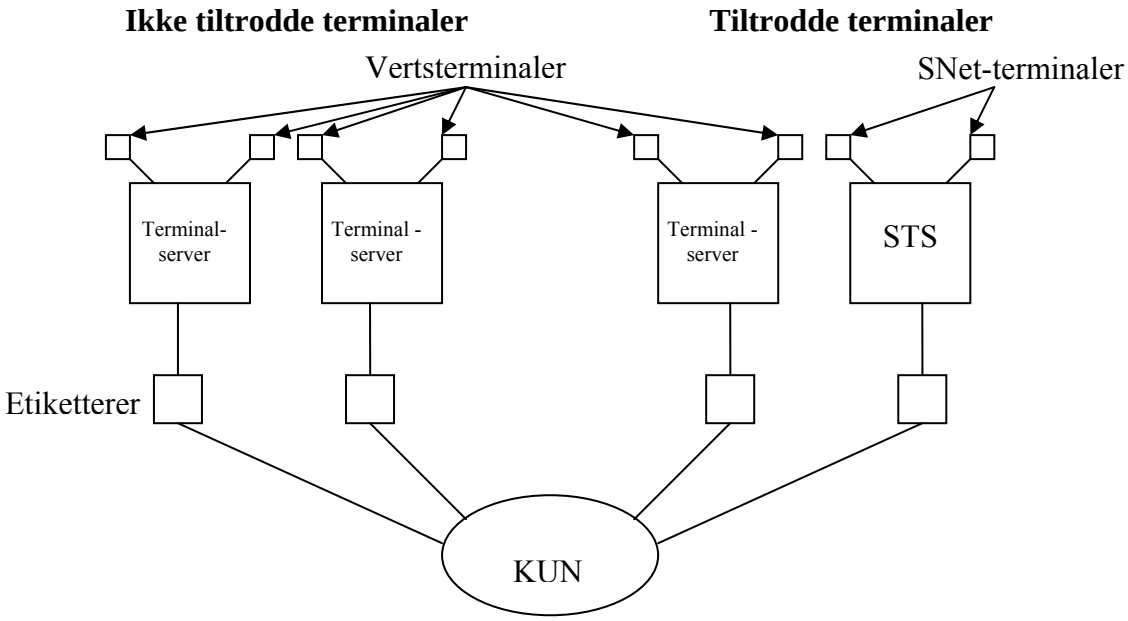
Målet med sikkerhetsmodellen er å lage en helhetlig modell som inneholder den sikkerhetspolitikken som et militært meldingssystem må ha. Vi kan bruke PBS, som et eksempel. PBS er et system som med stor sikkerhet er bygget på en tilsvarende modell som den Landwehr et al.(1984) presenterer. Sikkerhetsmodellen til Landwehr et al.(1984) er laget for å la brukere forstå sikkerhet i sammenheng med meldingssystemer. Modellen er utviklet som en guide til utviklingen av nye militære meldingssystemer, og den skulle bidra i evalueringen av slike systemer. Det kan virke som om at modellen har vært en god veiledning for mange, da den ofte blir trukket frem i forbindelse med utvikling av andre systemer.

5.2.7 SNet-modellen

Introduksjon og motivasjon

Glasgow og MacEwen (1987) presenterer en modell som skal brukes i et MLS distribuert system kalt SNet. Den første presentasjonen av arbeidet til Glasgow og MacEwen, ble holdt på en sikkerhetskonferanse i Gaithersburg i 1984. Den modellen de presenterte da, var en svært konkret og kompleks modell. De bestemte seg for å forenkle designet av modellen og delte den inn i to abstraksjonsnivåer. Glasgow og MacEwen (1987) har presentert en fullstendig spesifikasjon for begge lagene, der de fokuserer på selve modellen og dens matematiske fundament. Vi har bestemt oss for bare å vise den abstrakte, for å forenkle modellens egenskaper.

SNet



Figur 10: SNet arkitektur (Laget ut ifra Glasgow & MacEwen, 1987).

SNet er ifølge Glasgow og MacEwen (1987): *"SNet is a multilevel secure system in which a set of computers are connected via a network. Each computer, called a host, is either trusted or untrusted; trusted hosts are themselves multilevel secure systems that enforce an unspecified security policy, whereas untrusted hosts are systems that enforce no security policy. The essential idea is that an untrusted host can be used to store information of a common security level. (The incorporation of general-purpose trusted hosts in SNet is a byproduct of the design, a fact that is seen a little more clearly below.) Any one of the hosts can be accessed from any one of a set of trusted SNet terminals, which are trusted in the sense that it is assumed here that users of SNet are trusted. Host-only terminals allow a user access only to the host to which the terminal is attached and not to other SNet hosts (other than indirectly via its connected host operating system, of course). The particular security policies enforced by the trusted hosts are not specified, except for one particular host called the Secure Terminal Server (STS) to which the SNet terminals are attached. The STS is explained further below. Other trusted hosts may perform special security functions such as secure downgrading."* (Glasgow & MacEwen, 1987, s. 154).

I figuren over er alle vertene tilkoblet et ikke tiltrodd kommunikasjonsundernettverk (KUN) via et tiltrodd nettverksgrensesnitt kalt en etiketterer. Hver beskjed får en etikett av etiketteren, og den sier noe om hvilken gradering det er på informasjonen i meldingen. Denne etiketten blir brukt til å bestemme om beskjeden kan sendes videre til mottakeren. I følge Glasgow og MacEwen (1987) er det mest karakteristiske med SNet at den tillater enveis kommunikasjon. SNet unngår med dette komplekse toveis protokoller, som ofte brukes i tilsvarende problemstillinger.

En sikkerhetsmodell for SNet må adressere to typer informasjonsflyter, lagringsflyter og skjulte flyter. Håndhevingen av lagringsflytene involverer tre sikkerhetskrav, mens håndhevingen av de skjulte flytene involverer fire sikkerhetskrav (Glasgow & MacEwen, 1987). SNet-sikkerhetsmodellen må adressere følgende sju sikkerhetskrav: Markering (labelling), meldingsflyter, integritet, autentisering, entydighet, ordrebevaring, og ruting.

Spesifikasjonsspråket

Glasgow og MacEwen (1987) har valgt å bruke et spesifikasjonsspråk for å gjøre modellen mest mulig intuitiv og enklest mulig. Språket heter Lucid. Metoden bruker et nettverk til å forklare flyten av meldinger gjennom et system. Restriksjoner i meldingsflyten i nettverket blir representert av et tilsvarende program som også er skrevet i Lucid. Resultatet er da en Lucidspesifikasjon som en kan bevise ved å bruke Lucids bekreftelsesregler.

Glasgow og MacEwens (1987) Lucidspesifiakasjon av SNet inneholder et øvre lag med den abstrakte modellen som tilslutter seg en del sikkerhetsregler, og et nedre lag med den konkrete modellen.

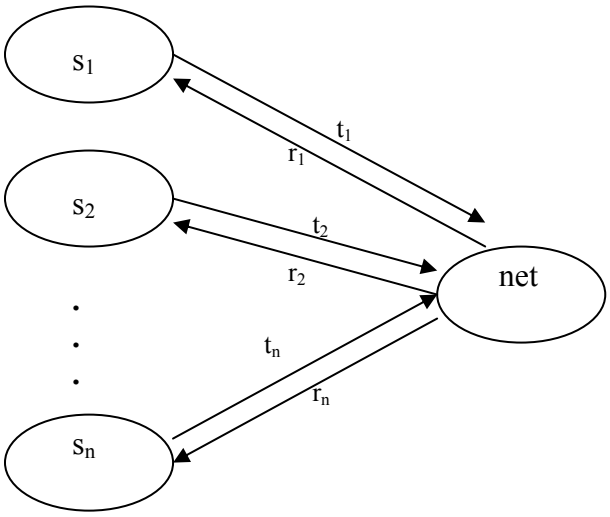
Syn på sikkerhet

SNet modellen til Glasgow og MacEwen (1987) modellerer flyt av informasjon mellom objektene. Under presenterer vi det øvre laget av sikkerhetsreglene som SNet modellen tilslutter seg.

Abstrakt modell

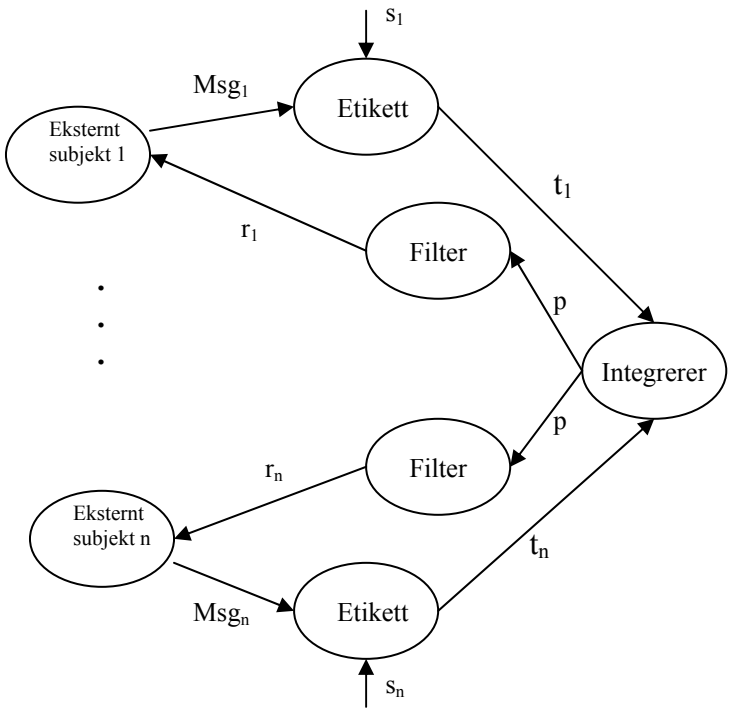
I begynnelsen av den abstrakte modellen presenterer Glasgow og MacEwen (1987) de fundamentale notasjonene til sikkerhet. Videre sier Glasgow og MacEwen (1987) at mengdene av subjektene utgjør både brukere og verter. Både brukerne og vertene bruker meldinger med data for å kommunisere. Transmisjoner av nye meldinger og kvitteringer av tidligere sendte meldinger er hendelser. En historie er et sett av par, der hvert par inneholder en uendelig sekvens av alle sendte og mottatte meldinger for et bestemt subjekt. Funksjonen Tiltrodd er en konstant som hovedsakelig spesifiserer om den kan eller ikke kan, bestemme etiketten på meldingen som blir sendt. I SNet er alle brukere og noen verter tiltrodde. For de ikke tiltrodde vertene blir etiketten på meldingen bestemt av funksjonen Maks nivå. Funksjonen Subjektnivå beskriver meldingsetiketten som er bestemt av de tiltrodde objektene. Funksjonene Meldingsnivå, Bestemmelsessted, Data og Sender definerer de fire feltene i en melding. Ny historie definerer en hendelse der den legger til en sendt melding inn i historie.

Lucid-spesifikasjonen for den abstrakte modellen



Figur 11: Et abstrakt operatørnett (Laget ut ifra Glasgow & MacEwen, 1987).

I figuren over illustrerer Glasgow og MacEwen (1987) den abstrakte sikkerhetsmodellen som et operatørnett. S_1, S_2, S_n og net er noder, mens pilene på figuren representerer historiesekvenser til meldinger som blir sendt mellom subjektene. Hver av disse pilene er merket med navnet til meldingssekvensen. Disse sekvensene blir så prosessert av nodene s_n og net.



Figur 12: Et raffinert abstrakt operatørnett (Laget ut ifra Glasgow & MacEwen, 1987).

I figuren over har Glasgow og MacEwen (1987) utvidet modellen et hakk ved at nodene net og $s_i (1 \leq i \leq n)$ er delt inn i to komponenter hver. For hvert subjekt s_i blir det definert en etikett som sikrer at riktig navn og nivå til sender er lagt ved alle sendte meldinger. I figuren er det også introdusert en ny meldingssekvens msg_i, som sender fra et eksternt subjekt n. Net-noden er oppdelt i en integrerer og en filternode. Integrereren tar inn alle meldingssekvenser som er sendt fra subjektene for så å legge dem inn i en singel sekvens p. For hvert subjekt s_i, tar filter bort alle meldinger fra sekvens p som ikke er berettiget til s_i. Både etiketten og filternodene er funksjoner av nettverksetiketten.

Videre i den konkrete modellen viser Glasgow og McEwen (1987) hvordan de ulike konseptene i den abstrakte modellen relateres til operasjoner. Operasjonene skal bli utført eksternt gjennom et visuelt brukergrensesnitt av agentdatamaskiner, brukerdatamaskiner og vertsdatamaskiner. Den største konkretiseringen Glasgow og McEwen (1987) har gjort i forhold til den abstrakte modellen, er at alle brukerbeskjeder inneholder en kommando.

Tanker rundt modellen

Dette er som sagt en spesifikk modell for et spesifikt system, og mange av egenskapene i SNet vil av den grunn ikke fungere for andre MLS-nettverk. Glasgow og MacEwen (1987) presenterer ikke noen passende verktøy for å utføre eller bevise Lucid-spesifikasjonene. Dette ser vi også på som en svakhet for modellen. Vi har heller ikke funnet noen konkrete bevis på at modellen er blitt brukt for det formålet den er tenkt til.

5.2.8 A Multilevel Security Policy Model for Networks

Introduksjon og motivasjon

Modellen er utarbeidet av Vijay Varadharajan (1990) og ble publisert i 1990. Varadharajan utviklet modellen ved Hewlett-Packard Laboratories i Storbritannia, og laget den ikke for et spesielt system. Slik vi ser det er Varadharajans (1990) arbeid ment å være en slags veiledning for utvikling av mer konkrete systemer. Vi har ikke funnet noe som tyder på at modellen noensinne har blitt implementert.

Modellen er en abstrakt nettverks-sikkerhetspolitikk-modell som adresserer noen av kravene som er beskrevet i The Trusted Network Interpretation (1987). Modellen betrakter krav til tilgangskontroll og informasjonsflytkontroll for et MLS-nettverk. Nettverks-tilgangskontroll-politikken fastsetter kravene for etablering av forbindelser mellom nettverkskomponenter og informasjonsflytpolitikken regulerer informasjonsflyten mellom nettverkskomponentene. Modellen brukes til formelt å bevise at kravene for tilgangskontroll ikke brytes og at informasjon ikke flyter fra høyere til lavere sikkerhetsklasser som et resultat av nettverksoperasjonene. Foruten selve modellen er også de tilhørende sikkerhetskravene formelt definert; videre er det utledet passende betingelser for at systemet skal tilfredsstille sikkerhetskravene. Hovedkonseptene som ligger til grunn for modellen er basert på en kombinasjon av flere kjente sikkerhetsmodeller: BLP-modellen (Bell & La Padula, 1973), MMS-modellen (Landwehr, Heitmeyer & Mclean, 1984), og Formal Models for Computer Security (Landwehr, 1981).
I tillegg til kravene vedrørende tilgangskontroll og informasjonsflyt, må kommunikasjonene beskyttes. På grunn av dette er det nødvendig med passende kryptografiske teknikker for å skaffe konfidensialitet, integritet og autentisering for kommunikasjonene. Varadharajan (1990) har ikke tatt slike kryptografiske teknikker i betraktning i sin beskrivelse av modellen.

Syn på sikkerhet

I første omgang beskriver Varadharajan (1990) designet av en nettverkssikkerhetsmodell. Nettverkstilgangskontrollpolitikken spesifiserer hvilke brukere eller prosesser som kan få tilgang til hvilke nettverkskomponenter. Ytterligere egnet informasjonsflytpolitikk må håndheves for å hindre ulovlig informasjonsflyt mellom ulike elementer. Av den grunn utfører Network Trusted Computer Base (NTCB) følgende to primærfunksjoner: *"1) Controlling the establishment of a connection between network entities, og 2) Regulating the flow of information between network entities"* (Varadharajan, 1990, s. 713).

Sikkerhetsmodellen er en tilstandsmaskinbasert modell, som i hovedsak beskriver et system som en samling av uavhengige objekter og verdier. Ved ethvert tidspunkt har objektene og verdiene en bestemt mengde relasjoner. Denne mengden med relasjoner utgjør tilstanden til systemet. Hvis relasjonen endres, endres også systemets tilstand. Den vanligste analysen man kan gjøre ut ifra en slik modell, er i følge Varadharajan (1990), grafanalysen for oppnåelighet.

Denne brukes til å avgjøre hvor vidt et system vil nå en viss tilstand eller ikke. Man kan for eksempel identifisere en delmengde av tilstander som representerer usikre tilstander. Hvis systemet oppnår en tilstand i denne delmengden, betegnes systemet som usikkert.

For å beskrive en tilstandsmaskinorientert sikkerhetsmodell må en på forhånd definere sikkerhetsrelaterte tilstandsvariabler, krav til sikker nettverkstilstand, samt nettverksoperasjoner som beskriver systemets tilstandsskifte. For å vise at et system i modellen er sikkert, må en vise at hver operasjon opprettholder sikkerhetskravene og at initialnettverkstilstanden er sikker.

Sikkerhetsantagelser

Nettverksmodellen lager i følge Varadharajan (1990) følgende sikkerhetsantagelser:

1. Pålitelige autentiseringsskjemaer for brukerne finnes inne i en verts nettverkskomponent. Alle brukere og prosesser i nettverket har unike identifikatorer.
2. Bare brukere med rolle som nettverkssikkerhetsansvarlig, kan tildele sikkerhetsklasser til subjekter og komponenter, og roller til brukere. En vertskomponent antas å ha et utvalg med sikkerhetsklasser å operere i.
3. Alle eksistenser i nettverksmodellen har sammenlignbare sikkerhetsklasser.
4. Pålitelig overførsel av informasjon på tvers av nettverket.
5. Hensiktsmessige kryptografiske teknikker er inkorporert i nettverkets tiltrodde database, som beskytter informasjonen før overførsel i nettverket. Disse kryptografiske målene er ikke tatt med i modellen.

Sikker tilstand

For å definere betingelser for at en tilstand skal kunne betegnes som en sikker tilstand, må en først bestemme hvilke faser systemet går igjennom i løpet av en operasjon. Dette gjelder Login Phase, Login Constraint, Connect Phase og Connect Constraint. Andre forhold som må taes hensyn til er i følge Varadharajan (1990), at klassifiseringen av informasjonen som kan sees gjennom en input-output-innretning ikke må være høyere enn klassifiseringen for innretningen, og at rollen til brukerne i en tilstand tilhører mengden med autoriserte roller.

Operasjoner

Varadharajan (1990) har satt opp et utvalg av operasjoner i modellen, og definert hva som kreves for at de skal være sikre. Dette gjelder blant andre Connect Operation og Information Manipulation Operations. Det kan være nødvendig å utvide denne listen til å inkludere andre operasjoner og utlede egnede betingelser for at disse operasjonene skal bli sikre. En eller en sekvens av operasjonene i modellen brukes blant annet av en aksjonsfunksjon for å beskrive overgangen når systemet går fra en tilstand til en annen.

Verifisering

For å verifisere sikkerheten i nettverkssystemet modellen beskriver, har Varadharajan (1990) gått nøye igjennom alle funksjonene i systemet og forsikret at systemet tilfredsstiller alle påkrevde sikkerhetsegenskaper. Verifiseringsprosessen er beskrevet ved en gjennomgang av de tre fasene: Login Phase, Connection Phase og Information Manipulation Phase. Ut fra dette har Varadharajan (1990) kommet frem til et sikkerhetsteorem for modellen, der det vises formelt når systemet er sikkert.

Tanker rundt modellen

Modellen er en slags kombinasjonsmodell som modellerer både flyt av informasjon mellom, og tilgangskontroll til objektene. Dette er den siste modellen vi har tatt med som omhandler tilgangskontroll.

Modellen er en slags hybrid mellom flere kjente modeller. Vi har tidligere i oppgaven presentert BLP-modellen og MMS-modellen, som danner grunnlaget for Varadharajans modell. Vi ser klare likheter med BLP og MMS i modellen til Varadharajan. Blant annet likner sikkerhetsantagelsene til Varadharajan svært mye på antagelsene i MMS-modellen. Det er tydelig at Varadharajan har tatt det beste fra hver modell, og endt opp med en modell basert på de gamle klassikerne.

5.2.9 An Execution Model for Multilevel secure Workflows

Introduksjon og motivasjon

Atluri, Huang og Bertino presenterte i 1997 An Execution Model for Multilevel secure Workflows. Dette er som tittelen sier, en modell som fokuserer på sikker arbeidsflyt. Modellen er ikke laget med tanke på et spesielt system, men mer for å veilede konstruksjonen av fremtidige systemer. Etter det vi vet, har det ikke blitt implementert systemer basert på denne modellen.

I en MLS sikker arbeidsflyt kan aktivitetene høre til forskjellige sikkerhetsnivåer. Sikring av oppgavebindinger fra oppgaver på høyere sikkerhetsnivåer til de på lavere sikkerhetsnivåer, kan gå på akkord med sikkerheten.

Atluri et al. (1997) sier at riktig utførelse av en MLS-arbeidsflyt krever at alle oppgavebindinger gjennomføres. Det er imidlertid vanskelig å sikre høy-til-lav-bindinger på grunn av konflikter mellom sikkerhet og nøyaktighet. Atluri et al. (1997) presenterer hvordan en MLS-arbeidsflyt kan utføres på en sikker og nøyaktig måte. Tilnærmingen er basert på semantisk gradering av oppgavebindinger som undersøker kilden til oppgavebindingene. Videre presenterer de algoritmer for automatisk omforming av arbeidsflyter på en slik måte at alle oppgavebindinger kan utføres uten å gå på akkord med sikkerheten.

I følge Atluri et al. (1997) er konklusjonene direkte anvendelige for andre relevante forskningsområder, som utførelse av flernivås transaksjoner i MLS-databaser, siden betydningsmessige krav kan modelleres i en arbeidsflyt.

Modellen

Først presenterer vi grunnelementene i arbeidsflytmodellen, og deretter følger en oppsummering av sikkerhetsmodellen som forutsettes.

Arbeidsflytmodellen

Atluri et al. (1997) definerer en arbeidsflyt som et sett av oppgaver med oppgavebindinger seg imellom. En oppgave består av et sett med dataoperasjoner og oppgaverotord, for eksempel begin, abort eller commit. Utførelse av en oppgave krever påkalling av disse oppgaverotordene, i tillegg til å påkalle operasjonsprosedyrer for dataelementer, enten read eller write. Alle dataoperasjoner i en oppgave må utføres etter at begin er utstedt, og alle oppgaver må avsluttes enten med commit eller abort.

En oppgave (t_i) kan i følge Atluri et al. (1997) være i en av følgende tilstander: initial state, execution state, commit state eller abort state. Videre kan et rotord flytte en oppgave fra en tilstand til en annen. For eksempel kan en oppgave flyttes fra initial tilstand til execution tilstand ved å påkalle rotordet begin.

Atluri et al. (1997) sier at oppgavebindinger i rekkefølge kan være enten statiske eller dynamiske. Hvis rekkefølgen er dynamisk er arbeidsflyten på forhånd definert i forhold til den aktuelle utførelsen. Dynamiske bindinger utvikler seg derimot i takt med at arbeidsflyten går fremover i utførelse. Oppgavebindinger kan eksistere blant oppgaver inne i en arbeidsflyt og betegnes som intra-workflow, eller mellom to ulike arbeidsflyter og betegnes som inter-workflow. Atluri et al. (1997) forklarer og drøfter til sammen fire ulike bindingskategorier for arbeidsflytmodellen: kontrollflytbindinger, verdibindinger, eksterne bindinger og kontrollflytbindinger med dataflyt.

Syn på sikkerhet

Atluri et al. (1997) antar at sikkerhetsstrukturen er en delvis ordnet mengde, som er bestående av forskjellige sikkerhetsnivåer. Videre deler Atluri sikkerhetsmodellen inn forskjellige klasser der en klasse $s_i \in S$ sies å være dominert av en annen klasse $s_j \in S$ hvis $s_i \leq s_j$. En klasse s_i sies å være strengt dominert av en annen klasse s_j (angitt som $s_i < s_j$)hvis $s_i \leq s_j$ og $i \neq j$.

Videre sier Atluri et al. (1997) at D er mengden av alle dataobjekter, der hvert dataobjekt $d \in D$ forbindes med et sikkerhetsnivå. Hver oppgave t_i i en arbeidsflyt W er knyttet til et sikkerhetsnivå, og det finnes en funksjon L som knytter alle dataobjekter og oppgaver til

sikkerhetsnivåer. I følge Atluri et al. (1997) kreves det at hver oppgave følger to sikkerhetsegenskaper, den enkle sikkerheten og den strenge egenskapen:

1. En oppgave t_i kan lese et dataobjekt bare hvis $L(d) \leq L(t_i)$
2. En oppgave t_i kan skrive et dataobjekt bare hvis $L(d) = L(t_i)$

I tillegg til disse to restriksjonene, må et sikkert system beskytte illegale informasjonsflyter via skjulte kanaler.

MLS-arbeidsflyter

En MLS-arbeidsflyt kan bestå av ulike sikkerhetsnivåer. Følgelig består en MLS-arbeidsflytmodell av noder på forskjellige sikkerhetsnivåer, der bindingene kan kobles til oppgaver på tilsvarende sikkerhetsnivå eller andre sikkerhetsnivåer. En binding som kobler seg mot oppgaver på samme sikkerhetsnivå kalles en intra-level-binding, mens en binding som kobler seg mot oppgaver på forskjellige nivåer kalles en inter-level-binding. Atluri et al. (1997) retter fokuset mot inter-level-bindinger, som igjen kan deles inn i to kategorier, høy-til-lav-bindinger og lav-til-høy-bindinger.

Semantisk gradering av oppgavebindinger i MLS-arbeidsflyter

I det videre arbeidet betrakter Atluri et al. (1997) alle typer bindinger og gjennomgår hva de semantisk betyr i et MLS-miljø. For å vurdere betydningen av høy-til-lav-bindinger, vurderer de først bakgrunnen for de ulike bindingene og kategoriserer de som følger:

1. *"The first category of dependencies arises to force the order of (conflicting) operations on shared data objects"* (Atluri, Huang & Bertino, 1997, s. 7).
2. *"The second category of dependencies arises to force properties such as atomicity, mutual exclusion, etc"* (Atluri, Huang & Bertino, 1997, s. 7).

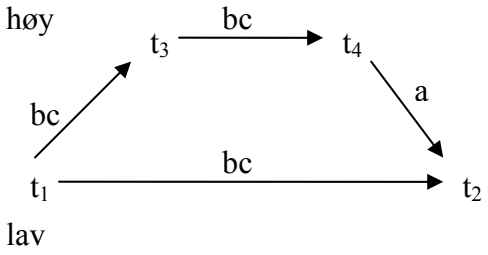
Videre bruker Atluri et al. (1997) oppgavebindingen fra eksempel 1, $t_2 \rightarrow t_3$, og forklarer at intensjonen for denne bindingen er å hindre overskriving av n og o med t_3 før t_2 leser dem. Av denne grunn er bakgrunnen for denne bindingen å fremme en spesiell ordre for de uoverensstemmende operasjonene, og tilhører derved den første kategorien. Bindinger i den andre kategorien er i følge Atluri et al. (1997) spesifisert i samsvar med betydningen av arbeidsflyten. Eksempelet under illustrerer slike bindinger i et MLS-miljø.

Eksempel: Oppgavebindinger i MLS-arbeidsflyt

Atluri et al. (1997) benytter et eksempel der en arbeidsflyt setter opp en reiseplan for en person P. P må først reise fra Washington D.C. til Toronto, og så fra Toronto til Moskva. Den siste delen av reisen er et hemmelig oppdrag og må derfor behandles som høyst sensitiv informasjon og krever derfor høyt nivå. Den første delen av reisen er imidlertid ugradert og behandles på lavt nivå. Arbeidsflyten består av i alt fire oppgaver: reservering av billett for den første delen av turen (t_1), kjøp av billett for den første delen (t_2), reservering av billett for den andre delen av turen (t_3) og kjøp av billett for denne (t_4). t_1 og t_2 karakteriseres som oppgaver på lavt nivå, mens t_3 og t_4 på høyt nivå.

Kjøp av en billett kan ikke starte hvis ikke reserveringen av billetten er fullført. Derfor $t_1 \rightarrow t_2$ og $t_3 \rightarrow t_4$. Videre kan reservering for den andre delen av reisen kun foretas etter at å ha fått bekreftet ledig plass for den delen av reisen som er lav, så $t_1 \rightarrow t_3$. Det er også slik at hvis kjøp av billett for den andre delen av reisen mislykkes, må billetten for den første delen av reisen også kanselleres, så $t_4 \rightarrow t_2$. Mens de to første oppgavebindingene er intra-level-bindinger, er de to siste henholdsvis en lav-til-høy-binding og en høy-til-lav-binding.

Intensjonen for høy-til-lav-bindingen $t_4 \rightarrow t_2$, er å samle betydningen av arbeidsflyten mer enn å presse frem en ordre mellom uoverensstemmende operasjoner. Av denne grunn tilhører denne bindingen den andre kategorien.



Figur 13: Eksempel: Oppgavebindinger i MLS-arbeidsflyt (Laget ut ifra Atluri et al., 1997).

Atluri et al. (1997) betegner bindingene i første kategori som conflicting (CN), og bindingene i andre kategori betegnes som result-dependent (RD). Dette presenteres med formelle definisjoner i artikkelen. Videre følger også formelle definisjoner for bindinger som er conflict-free (CF) og result-independent (RI). Vi har valgt å ikke ta med definisjonene her, men viser figuren som er et resultat av de nevnte definisjonene:

RD	Avbrutt (svak)	Avbrutt (svak) Ikke avbrutt (sterk og svak)
RI	Ikke avbrutt (sterk og svak)	ϕ
	CN	CF

Figur 14: Kategorisering av high-to-low-bindinger (Laget ut ifra Atluri et al., 1997).

Atluri et al. (1997) sier at ideen bak denne klassifiseringen er at resultatet av utførelsen av enten barnet (hvis RD) eller forelderen (hvis CN), må være forskjellig avhengig av om bindingen er tvunget igjennom eller ikke. Det kan følgelig ikke være bindinger som er både

CF og RI. Denne kategoriseringen av høy-til-lav-bindinger er viktig fordi hver kategori må behandles i henhold til ulike tilnærminger i et MLS-miljø.

Utførelse av MLS-arbeidsflyter

I følge Atluri et al. (1997) vil ikke en utførelse av en lav-til-høy-binding resultere i brudd på sikkerheten. Derimot kan en skjult kanal etableres mens en høy-til-lav-binding utføres. Høy-til-lav-bindingene er derfor mye vanskeligere å håndtere enn lav-til-høy-bindingene.

Videre sier Atluri et al. (1997) at siden CN-RI-bindinger er uoverensstemmende, er spørsmålet hvordan en kan synkronisere oppgavene for å tilfredsstille bindingen uten å introdusere skjulte kanaler. Tilnærmingen for å behandle CN-RI-bindinger eliminerer høy-til-lav-bindingen ved å dele opp oppgaven som er høy. Formålet med en CF-RD-binding er å tvinge en lav oppgave inn i en spesiell tilstand i samsvar med tilstanden for den høye oppgaven. Tilnærmingen for å håndtere CF-RD oppveier for den lave oppgaven ved å utføre en invers oppgave når det er nødvendig. Den siste bindingen er en CN-RD som en kombinasjon av CN-RI og CF-RD siden den kan være forårsaket av uoverensstemmende operasjoner så vel som betydningene av arbeidsflyten.

Tanker rundt modellen

Dette er den eneste rene arbeidsflytmodellen vi har tatt med i oppgaven. Modellen presenterer som en MLS-arbeidsflyt, og viser hvordan arbeidsflyten kan gjennomføres i praksis.

En organisasjon som Forsvaret utfører mange arbeidsflyter daglig. Kanskje kan modellen benyttes i SAP DEIG, i forbindelse med arbeidet med å implementere MLS i SAP? Det negative med modellen er at den ikke dreier seg om et fullverdig MLS-system. Likevel mener vi at den kan bidra til en helhetsforståelse for hvordan MLS-arbeidsflyter kan bygges opp, og derfor være nyttig for blant annet SAP DEIG.

5.2.10 MLS Workflow Management System

Introduksjon og motivasjon

USAs militære Naval Research Labratory (NRL) startet på nittitallet et utviklingsprosjekt for å bygge en MLS Workflow Managment System (WFMS). Grunnlaget for dette prosjektet var å utvide mulighetene for en vanlig WFMS. På den tiden støttet ikke en vanlig kommersialisert arbeidsflyt distribuerte oppdragskritiske applikasjoner. De håndhevet ikke aksesskontrollpolitikker, og da heller ikke flernivåsikkerhet. NRL bestemte seg da for å utvikle verktøy og sikkerhetskritiske komponenter som skulle endre på dette. Personene som fikk oppgaven var Kang, Froscher, Eppinger og Moskowitz. Strategien deres skulle overholde to mål der det ene var at de skulle ha en maksimal bruk av kommersiell software og hardware, og det andre var at et MLS WFMS skulle ha en sikker flyt mellom oppgaver på forskjellige

klassifiseringsdomener. For å klare dette trengte de noen ikke-kommersialiserte komponenter, og de utviklet da blant annet NRL pump, som vi har beskrevet tidligere i kapittel 2.2.4.

For å nå målene valgte Kang, Froscher, Eppinger og Moskowitz å bruke den multiple singlenivåarkitekturen som er beskrevet i Kang, Froscher, og Moskowitz sin artikkel fra 1997, An Architecture for Multilevel Secure Interoperability, og i Kang, Froscher, og Eppingers artikkel fra 1998, Toward an Infrastructure for MLS Distributed Computing. Denne arkitekturen danner grunnlaget for håndhevelsen av informasjonsflytkravene.

Kang, Froscher, Eppinger og Moskowitz (1999) presenterer kravene til MLS-arbeidsflyter, verktøyer for å støtte MLS-arbeidsflyter, og en strategi for å implementere dem.

Strategivalg

Strategien Kang et al. (1999) valgte, var at MLS WFMS skulle fungere som en vanlig WFMS. Dette ville de oppnå ved å ha singlenivås oppgaver. Oppgaver kan være singlenivå individuelt, men de kan være lokalisert i forskjellige klassifiseringsdomener, og må da samarbeide for å oppnå et høyere nivå.

Kang et al. (1999) lagde videre noen krav som informasjonsflyten måtte oppfylle:

- Høyere nivåers brukere må ha tilgang til lavere nivåers data og lavere nivåers ressurser.
- Høyere nivåers prosesser må ha tilgang til lavere nivåers data.
- Høyere nivåers data må ikke lekke informasjon til lavere systemer og brukere.

For å håndheve disse kravene betraktet de hvordan Atluri, Huang og Bertino (1997) hadde gjort det. De fant to måter for å håndheve MLS-reglene i et MLS-arbeidsflytsystem:

1. Bygg en høyt sikret MLS WFMS som vil kjøre på en MLS-plattform, eller
2. Bygg en MLS-arbeidsflyt ved å integrere flere singlenivås arbeidsflyter med en MLS-distribuert arkitektur.

Kang et al. (1999) visste at det første alternativet hadde vært prøvd før, og at det hadde vært en svært teknisk utfordrende og dyr utviklingsmetode. På grunn av dette valgte Kang et al. (1999) å gå for den andre løsningen med den arkitekturiske metoden.

Kang et al. (1999) valgte følgende tekniske tilnærming:

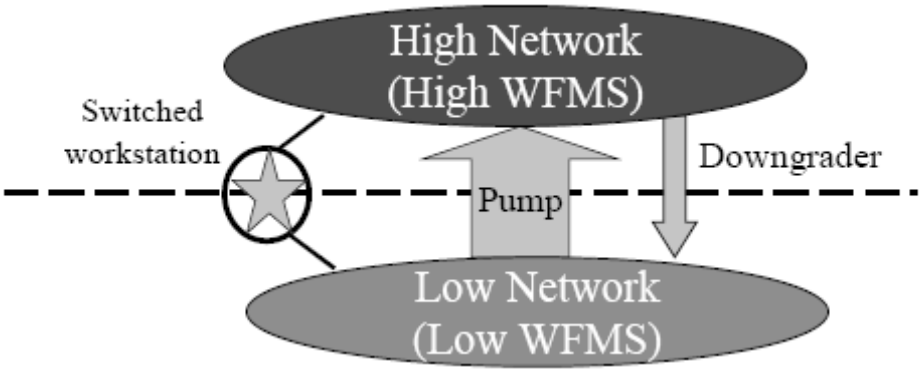
- Velg en MLS-distribuert arkitektur der flere singlenivås arbeidsflyter kan bli utført.
- Velg en strategi for å dele opp en MLS-arbeidsflyt inn i flere singlenivås arbeidsflyter.
- Velg et singlenivå WFMS som kan utføre singlenivås arbeidsflyter i hvert graderingsdomene.
- Implementer de nødvendige verktøyene som støtter en MLS-arbeidsflyt

- Utvid arbeidsflytsamarbeidsmodellen slik at den tilpasser seg kommunikasjonen mellom forskjellige graderingsdomener.
- Utvid arbeidsområdenes singlenivås arbeidsflyter, slik at de kan tilpasse seg kommunikasjon mellom oppgavene i forskjellige graderingsdomener.

Et stort problem når en skal ha flere single arbeidsflyter, er å få dem til å samarbeide. Samspillevne mellom arbeidsflytene er et svært viktig krav hvis en skal få til en MLS-arbeidsflyt. Det er i følge Kang et al. (1999) to viktige aspekter som må til for å oppnå samspillevne i arbeidsflytene: å ha en samspillevneprotokoll mellom forskjellige WFMS, og at det er mulig å modellere samspillevne i en arbeidsflyts prosesseringsverktøy.

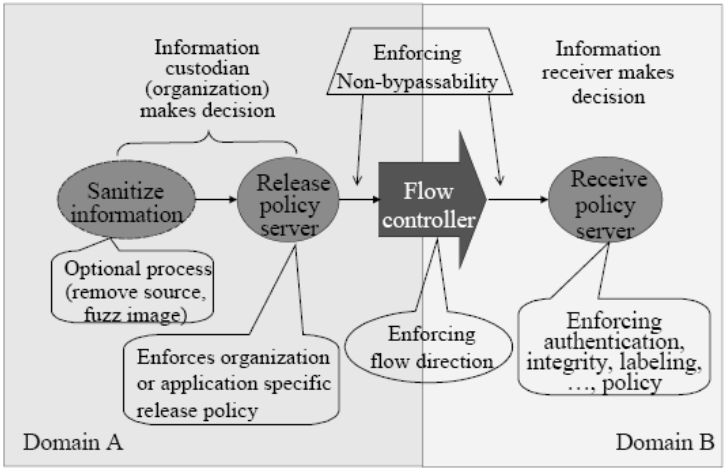
Syn på sikkerhet

I en distribuert arkitektur stoler ikke MLS-arbeidsflyten på singlenivå WFMS, men heller på den underliggende MLS-distribuerte arkitekturen. Den MLS-distribuerte arkitekturen vil i følge Kang et al. (1999): være vert for flere singlenivå arbeidsflyter som skal bli utført, og forsyne kanaler slik at informasjon kan passere mellom oppgaver i ulike graderingsdomener.



Figur 15: En MLS distribuert arkitektur (Kang et al. , 1999).

De svitsjede arbeidsstasjonene lar brukere aksessere ressursene og lage informasjon i de ulike domenene som brukeren har autorisasjon for. Enveis innretninger sammen med informasjonsfrigivelse og mottakspolitikkservere, gjør det til en sikker måte å sende informasjon mellom forskjellige graderingsdomener på.



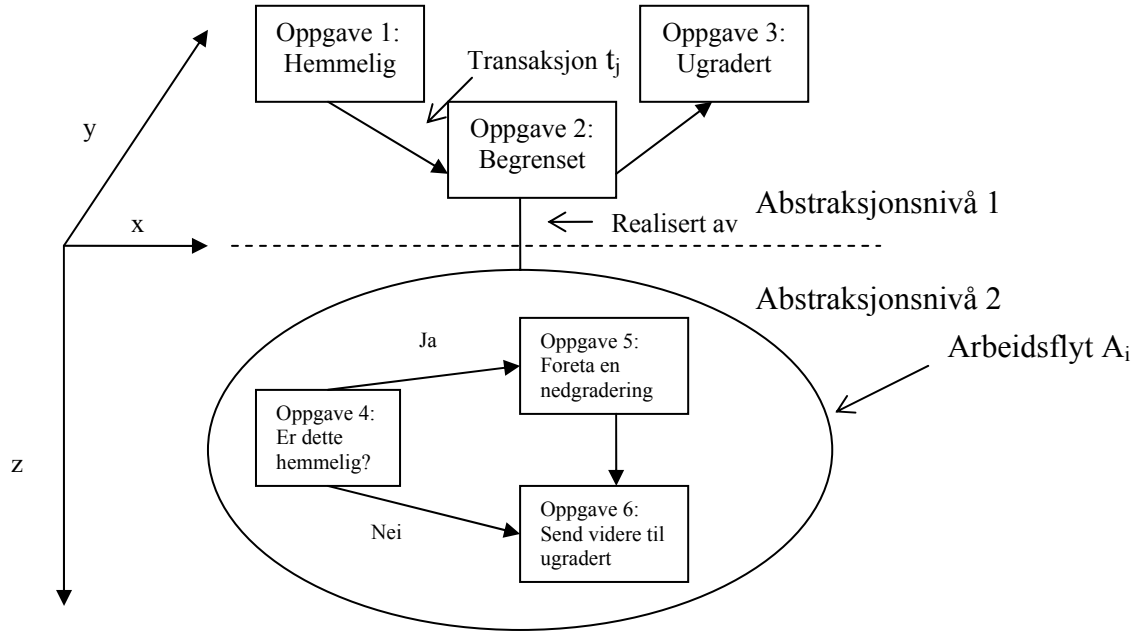
Figur 16: Informasjons-, frigivelse-, og mottakspolitikker (Kang et al., 1999).

En informasjonsfrigivelsesserver oppholder seg i et klassifikasjonsdomene der informasjonen er frigitt, mens en informasjons-mottaks-politikk-server på en sikker måte skaffer informasjon fra et klassifiseringsdomene til et annet. Et eksempel på en distribuert WFMS kan være ORBWork (Kochut, Sheth & Miller, 1998) som er en spesifikk versjon av METEOR (Meteor).

MLS WFMS-modellen

Strategien for implementeringen som Kang et al. (1999) har valgt, er å kombinere ulike singlenivås arbeidsflyter på en distribuert arkitektur. De har brukt METEOR WFMS (Meteor) som singlenivå WFMS. Grunnen til dette valget er ifølge Kang et al. (1999) at METEOR WFMS er CORBA-kompatibel og samtidig distribuert. Kang et al. (1999) har måttet modifisere modellen for MLS-arbeidsflyt. Nedenfor presenterer vi den modifiserte modellen som Kang et al. (1999) har kommet frem til.

En oppgave er en abstraksjon av en aktivitet og kan sees på som en del av et arbeid som blir utført av ulike prosesseringsenheter. En oppgave kan bli utført av et individ eller av en datastyrt prosess som utfører et program. Det finnes to forskjellige typer oppgaver, en fremmed oppgave der utførelsen av oppgaven er ukjent og en naturlig oppgave der utførelsen av oppgaven er kjent. I tillegg kommer nettverksoppgaver som representerer kjernen av arbeidsflytaktivitetene.



Figur 17: Eksempel på en METEOR-modell.

Figuren over viser hvordan modellen kan fungere. Vi har tre klassifiseringsnivåer, HEMMELIG, BEGRENSET og ugradert. Hvis HEMMELIG nivå (Oppgave 1) skal sende noe til ugradert nivå (oppgave 2), blir oppgave en kildeoppgave og oppgave to bestemmelsesstedsoppgave. Det blir da en transaksjon t_j fra HEMMELIG til BEGRENSET, og en fra BEGRENSET til ugradert. Før transaksjonen fra BEGRENSET til ugradert starter, må noen oppgaver utføre overføringen av informasjon fra HEMMELIG til BEGRENSET. Disse oppgavene befinner seg da på abstraksjonsnivå to. BEGRENSET nivå får så en nettverksoppgave. Nettverksoppgaven er alltid assosiert til den oppgaven som er dens opphav, som i dette tilfellet er BEGRENSET. Arbeidsflyten W_i inneholder oppgavene fire, fem og seks. Oppgave fire skal sjekke om innholdet som blir sendt er HEMMELIG, oppgave fem skal nedgradere innholdet, og oppgave seks skal sende innholdet videre til ugradert. MLS METEOR-modellen kan betraktes som at oppgaver i forskjellige domener skjer i xy-planet, mens z-aksen representerer ulike nivåer av abstraksjon med tilhørende oppgaver.

Tanker rundt strategien

Prosjektet til Kang et al. (1999) har så vidt vi vet, ikke blitt realisert i noen militære organisasjoner. Vi tror det bare har blitt eksperimentelt testet, siden vi ikke har funnet noe dokumentasjon på noe annet. Vi har heller ikke funnet noe dokumentasjon på hvordan strategien har fungert eksperimentelt, hvilket kan være på grunn av at dette er gradert informasjon. Strategien er en interessant tilnærming, og den kan trolig være til hjelp til andre forskermiljøer.

5.2.11 Domain Based Security

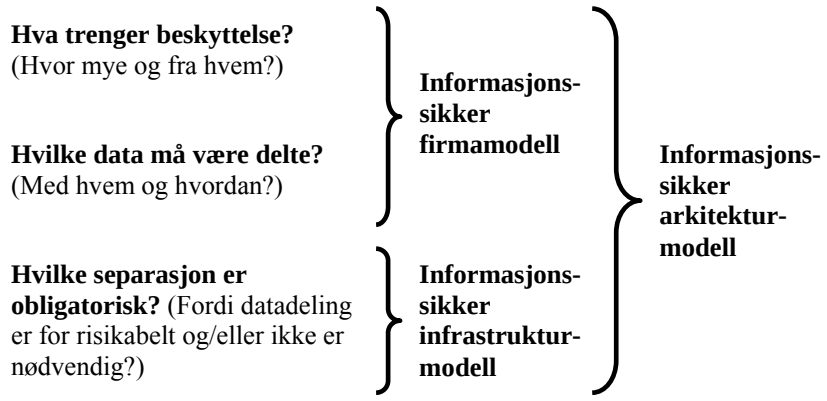
Introduksjon og motivasjon

Domain Based Security (DBSy) (Robinson, 2001; Hughes, 2002; Warrener, 2003) er ikke en modell, men en metode for å møte informasjonssikkerhetskrav innen forretningsvirksomhet. DBSy ble opprinnelig utviklet av DERA for United Kingdom Ministry of Defence i 2000, men fra juli 2001 ble DERA splittet i to organisasjoner, dstl og QinetiQ. Sistnevnte fikk ansvaret for å videreformidle metoden.

DBSy er en pakke med konsepter, metoder og teknikker som er designet for å møte kravene til moderne informasjonssystemer, som støtter reelle sikkerhetskrav. Metoden og teknikkene kan brukes i alle organisasjoner som har behov for å skreddersy et IT-system til gjeldende sikkerhetskrav. Metoden DBSy gir system-til-system-sikkerhet.

I følge Huges (personlig kommunikasjon, 28. april 2005) gir metoden og teknikkene en relevant analyse av sikkerhetsrisikoene som er assosiert med MLS.

En bruker kan sende en melding til en domenegrense ved å bruke domenets arveteknologi. Deretter vil domenegrensesystemet verifisere sikkerheten og gi den riktige sikkerheten til endestasjonssystemet for meldingen. Metoden greier dette ved å bruke avansert kommersialisert sikkerhetsteknologi.



Figur 18: Informasjonssikre kravmodeller (Laget ut ifra Robinson, 2001).

DBSy bruker en grafisk modelleringsteknikk for å definere en sikkerhetsarkitektur for en organisasjon. Teknikken definerer først en informasjonssikker firmamodell, som er en grafisk representasjon av de nødvendige firmakoblingene. En kobling beskriver firmaets beskyttelse og delingskrav. Firmamodellen viser hvilke behov firmaet har for deling av informasjon mellom ulike grupper innad i firmaet. Det blir videre laget en informasjonssikker infrastrukturmodell som viser hvordan den informasjonssikre firmamodellen er implementert av IT-infrastrukturen. Disse to modellene kombineres deretter for å få en informasjonssikker arkitekturmodell. Denne modellen viser hvordan et firmas domener og koblinger av en

informasjonssikker firmamodell, er styrt av øyene og landeveiene til en informasjonssikker infrastrukturmodell.

Syn på sikkerhet

DBSy-metoden modellerer flyt av informasjon mellom domene og objektene. Dette gjøres ved at miljøene igjennom portalene sier hvilke domener som kan sende informasjon med hverandre. Informasjonen blir da sendt igjennom koblingene mellom domenene. Dette beskriver vi nærmere i neste kapittel.

Informasjonssikre firmamodeller

Den informasjonssikre firmamodellen setter som nevnt begrensningene for hvor mye brukerne av systemet kan dele foretakets data. Modellen har fire grunnelementer; domener, koblinger, miljø og portaler.

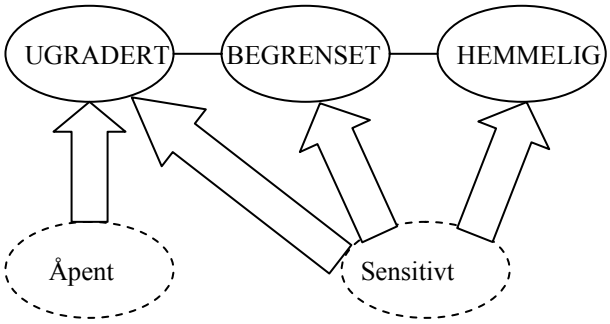
Figur 19: En enkel firmamodell.

- Domener: *"Domains represent the logical places where people work and exchange data by means of software acting on their behalf. The interesting property of a domain is not how the domain members share data within the domain, but rather the fact that between different domains sharing is either prohibited or only permitted in accordance with well-defined constraints."* (Robinson, 2001, s. 2). Et domene i DBSy kan være IT-systemer, en logisk gruppering av mennesker, ressurser, eller forskjellige foretaksfunksjoner.

- Koblinger: *"Connections provide the means of sharing data among members of different domains. Two domains are connected if data may be transferred from members of one domain to members of the other."* (Robinson, 2001, s. 2).

- Miljøer: *"Environments represent physical places where people work and where electronic media and equipment are located."* (Robinson, 2001, s. 2).

- Portaler: *"Portals provide the means by which domain members may interact with their domains. From an environment, there may be portals for several domains. Some people in the environment may be members of one or more of these domains, while others may not be members of any of them."* (Robinson, 2001, s. 2).

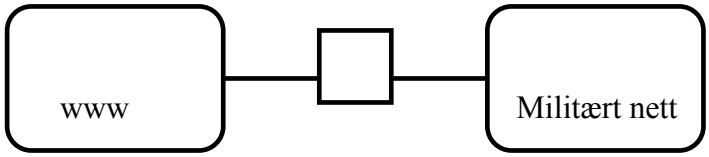


Figur 20: Modell som viser miljøene.

Eksempelet over viser miljø og portaler for et gitt firmadomene. Det er to miljøer, åpent og sensitivt, og fire portaler. Dette eksempelet viser at medlemmene i det ugraderte domenet enten kan jobbe i de sensitive eller de åpne miljøene, mens BEGRENSET og HEMMELIG domene bare kan jobbe i sensitive miljøer.

Informasjonssikre infrastrukturmodeller

Den informasjonssikre infrastrukturmodellen viser som sagt hvordan firmamodellen er implementert av IT-infrastrukturen. Modellen inneholder to grunnelementer, øyer og landeveier.



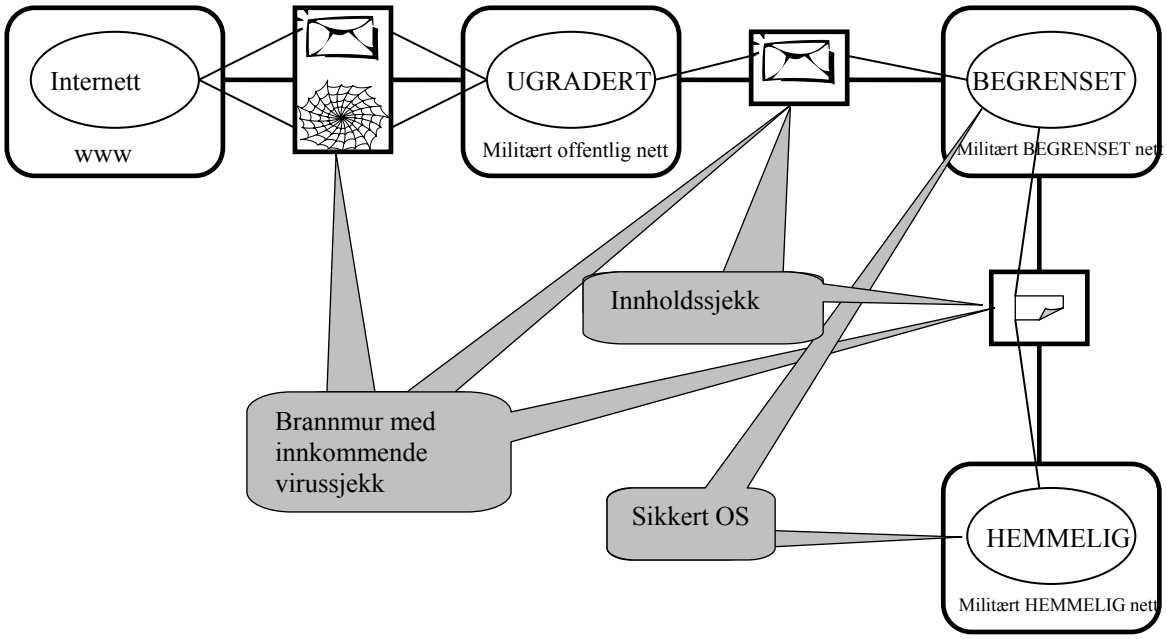
Figur 21: To infrastrukturøyer.

En øy er et datasystem som er separert fra alle andre datasystemer med en ugjennomtrengelig grense. En øy er representert av et tykt rektangel med runde hjørner, der navnet på øyen er i bunnen. En øy kan inneholde ingen, et eller flere domener. Øyene kan være spredt rundt i firmaet og sammenkoblet med landeveier (Robinson, 2001). Landeveiene er konstruert slik at de bare slipper igjennom en spesiell spesifisert kommunikasjon. Slik kommunikasjon kan være e-post, video, Internett-tilgang osv. (Robinson, 2001). Modellen over representerer infrastrukturen til et firma, www representerer her Internett, og firkanten mellom www og firmanettet kan være en spesifikk kommunikasjon som skal slippe igjennom.

Informasjonssikre arkitekturmodeller

Firmamodellen legger seg oppå infrastrukturmodellen, slik at firmamodellen blir støttet av hver øy med infrastruktur. Landeveiene implementerer koblingene mellom domenene som er på de forskjellige øyene. Resultatet er en informasjonssikker arkitekturmodell. Denne modellen gir en klar kartlegging mellom samhandlingene til firmaprosessene, mens kontrollene gir beskyttelse til kritisk og sensitiv informasjon (Warrener, 2003).

Figuren nedenfor illustrerer en informasjonssikker arkitekturmodell. Vi har bygget videre på eksempelet vi beskrev ovenfor: www verter Internettdomenet, mens de militære nettene verter hvert sitt sensitive domene, henholdsvis ugradert, BEGRENSET og HEMMELIG. Videre er det virussjekker og brannmurer mellom alle øyene, for å unngå uheldige situasjoner. HEMMELIG og BEGRENSET domene har også et sikkert operativsystem. Dette operativsystemet kan videre begrense domenebrukernes rettigheter, slik at de bare får tak i den informasjonen de trenger. Videre er det en innholdssjekk som kontrollerer innholdet i informasjonen som blir sendt mellom BEGRENSET- ugradert og HEMMELIG-BEGRENSET; dette for å hindre at sensitiv informasjon ikke blir sendt til et lavere nivå.



Figur 22: Eksempel på et domenebasert nettverk.

Tanker rundt metoden

DBSy-metoden har noen klart sterke sider. Den sterkeste er kanskje at den viser klart og tydelig et firmas behov for sikkerhet. Det vil si at det ser klart hvor det skal være høy sikkerhet og hvor det skal være lavere sikkerhet, uten å forstyrre firmaaktiviteten mer enn nødvendig. Metoden møter også reelle behov for et firma ved å bruke avansert kommersiell sikkerhetsteknologi, som er svært kostnadseffektivt i forhold til å lage sin egen teknologi. DBSy er veldig generell og kan implementeres nesten over alt og hvor som helst. Domener og øyer er som sagt, brukt for å skille ut ulike grupper av brukere i en organisasjon. Gruppene kan være forskjellige avhengig hva de skal gjøre. En gruppe kan for eksempel representere hæren, sjøforsvaret, luftforsvaret eller noe annet.

En svakhet ved metoden er at den ikke er noen formell modell. Videre gir den ikke et MLS-system, men snarere et Multiple-Single Level (MSL)-system. Den kan aldri alene kunne bli godkjent som et fullverdig MLS-system. En annen svakhet ved metoden er at den bruker

kommersialiserte produkter. Forsvaret ønsker vanligvis å ha spesielle systemer som er bygget spesifikt for dets behov. Dette med tanke på å senke kjennskapen til systemet. Med kommersialiserte produkter vil det alltid være utenforstående som har kjennskap til systemet, samt dets fordeler og ulemper. Dette kan utnyttes av personer med uedle hensikter, som kan få tilgang til systemet ved for eksempel å bruke en trojansk hest, eller ødelegge systemet ved å bruke et virus.

DBSy og Common Criteria

Den tradisjonelle tankegangen har alltid vært BLP-modellens kontroll av informasjonsflyt. CC og alle tidligere formelle modeller har ifølge Hughes (personlig kommunikasjon, 28.april 2005), bare tatt for seg håndheving av separasjon mellom de forskjellige nivåene. Den tradisjonelle tankegangen kan se ut til å endre seg med den nye metoden til QinetiQ, DBSy. Her ser en på sikkerheten på en annen måte; dette dreier seg om hvordan en kan få til kontrollert deling av informasjon mellom nivåene.

"The functions defined in Common Criteria (CC) do not readily fit the mould of DBSy. The focus for CC is on specification of functions, whereas DBSy is focussed on specifying required effects, which includes the effect of separation (or lack of functionality) as well as the actual functions themselves. Also, much of CC is concerned with 'information flow' properties based on the Bell-LaPadula model, which is a specification for achieving separation and is not concerned with controlled sharing of information. Hence there are features of DBSy that are specifically adapted to specifying the required effects of 'multi-level' security and which are entirely absent from CC." (Personlig kommunikasjon, Hughes, 28. april 2005).

Det kan by på utfordringer å evaluere et DBSy med CC, siden de ikke baserer seg på samme tankemåte. Det er mulig å evaluere et DBSy-system til EAL4. Høyere CC-sertifiseringer krever imidlertid en formell, matematisk bevist modell. Dette hindrer DBSy fra å kunne evalueres høyere enn EAL4.

Wiseman (personlig kommunikasjon, Wiseman, 29. april 2005), mener at CC-evalueringen bidrar lite til sikkerhet, og fokuserer på feil ting:"*It does not focus on what really matters, cannot reason about separation, cannot reason about content checking and is horribly expensive and overburdened with bureaucracy.*" (Personlig kommunikasjon, Wiseman, 29. april 2005).

5.2.12 Multilevel Security i dag og i fremtiden

Det finnes flere eksempler på realiserte MLS-systemer, men erfaringene er blandet. Ølnes påpekte at dette har med nødvendige sertifiseringer å gjøre, og at en ender opp med statiske systemer med meget kompliserte rutiner for oppgraderinger og feilrettinger. Dette gjør at brukervennligheten blir lav. Nedenfor har vi presentert noen eksempler på realiserte MLS-

systemer. Deretter har vi presentert løsninger med delvis MLS-funksjonalitet som benyttes i Forsvaret i dag. Til slutt har vi skrevet om videre arbeid innen MLS og kort om MSL som et alternativ til MLS.

Realiserte MLS-systemer

Blant de MLS-systemer som er realisert har vi valgt å presentere MLS Unix and Trusted Windowing, MLS logistikksystemer, en løsning fra IBM og SyBard. Det finnes flere andre eksempler, blant annet en gammel løsning fra Oracle. Denne er for øvrig ikke anvendbar, men en fullstendig MLS-løsning. Systemet er lukket og har ingen forbindelse ut. Videre presenterte Sun Solaris en løsning for mange år siden, Trusted Solaris v1.1. Denne ble evaluert til B1 i TCSEC, men denne løsningen er gammel og har dårlig brukergrensesnitt, og produseres ikke lenger. På grunn av dårlig funksjonalitet, har vi ikke presentert disse løsningene i rapporten.

MLS Unix og CMW

De fleste tilgjengelige MLS-systemer er modifiserte versjoner av Unix. Et eksempel er AT&T's System V/MLS (Amoroso, 1994), som la til sikkerhetsnivåer og etiketter, først ved å bruke noen av bitene i gruppen ID record og deretter ved å bruke dette til å spisse inn mot en mer forseggjort struktur (Anderson, 2001). Dette gjorde det mulig for MLS-egenskaper å bli introdusert med minimale endringer i systemkjernen. Andre produkter av denne typen inkluderte SecureWare og avledede produkter som SCO og HP VirtualVault, og Addamax.

CMWer tillater data på ulike nivåer å bli betraktet og modifisert samtidig av en menneskelig operatør, og forsikrer at etikettene som hører til informasjonen blir riktig oppdatert (Anderson, 2001). Dette egner seg for eksempel i etterretningsmiljøet, der analytikere har tilgang til TOP SECRET-data og produserer rapporter på SECRET-nivå. Disse rapportene er utsatt for å bli stjålet og må derfor ikke inneholde informasjon som kan avsløre etterretningskilder eller metoder. I følge Anderson (2001) tillater CMWer analytikere å se TOP SECRET-data i et vindu og å lage rapporter i et annet vindu, samt å ha mekanismer som forhindrer tilfeldig kopiering fra gamle til nyere data, for eksempel cut-and-paste fra SECRET til TOP SECRET, men ikke omvendt. CMWer har vist seg å være svært nyttige innenfor operasjoner og logistikk.

Logistikksystemer

Militære lagringsenheter som offentlige dokumenter, kan ha forskjellige graderingsnivåer. Noe sambandsutstyr er gradert STRENGT HEMMELIG, mens informasjon om flydrivstoff ikke er det. Informasjon om drivstoff kan imidlertid være HEMMELIG hvis mengden eller bevegelsene kan lekke informasjon om taktiske intensjoner. Videre kan for eksempel et navigasjonssystem som er gradert KONFIDENSIELT i fredstid, inneholde en laserstyrt gyroplattform som er gradert HEMMELIG i en krigssituasjon. Sikkerhetsnivåer er altså ikke monotone.

Systemene som trengs for å håndtere alt dette kan synes å være vanskelige å lage. I følge Anderson (2001) har MLS-logistikkprosjekter både i USA og Storbritannia endt opp som dyre katastrofer. RAF's LITS var et prosjekt for å utvikle et enkelt administrasjonssystem for RAFs åtti baser. Systemet var i henhold til Anderson (2001) designet til å operere på to nivåer: BEGRENSET for flydrivstoff og skokrem, og HEMMELIG for spesielt materiell som atomvåpen. Det ble opprinnelig implementert som to separate systemer sammenkoblet med en pumpe for å håndheve MLS-egenskapene. Prosjektet varte i ti år, 1989-1999, og hadde en prislapp på fem hundre millioner dollar. Prosjektet ble en klassisk historie om økte kostnader grunnet stadig nye krav om forandringer.

IBM

Liberg nevnte et system som IBM solgte til et farmasøytisk firma i 2003. Dette ble solgt som et MLS-system og er i stadig bruk. Dette systemet tilfredsstiller i likhet med andre realiserte MLS-systemer, ikke Forsvarets krav til sikkerhet, men vi har likevel valgt å presentere løsningen.

IBM samarbeidet med Winchester Business Systems, og laget et MLS-produkt til Fujifilm Medical Systems USA Inc. Det farmasøytiske firmaet måtte skifte system da de fant at papirsystemet ikke lenger tilfredsstilte dets behov.

De største utfordringene var styringsendringen. Hver gang et produkt, dokument eller spesifikasjon ble endret, måtte firmaet forsikre seg om at de nye versjonene ville fungere sammen med eldre modeller. Firmaet hadde også behov for å beherske gamle inventarlister og lagerbeholdninger.

Overholdelse av gjeldende bestemmelser fra myndighetene, nærmere bestemt The US Food and Drug Administration (FDA), var en annen kritisk utfordring (Fujifilm Medical Systems). Dette gjaldt regler vedrørende tilgang, kontroll og bruk av elektronisk opptak og elektroniske signaturer. Fujifilm Medical Systems måtte kunne garantere personvern i henhold til lover og regler overfor sine kunder.

Fujifilm Medical Systems trengte en løsning langt større enn bare et administrasjonsverktøy for dokumenter. For å hjelpe firmaet med å få bedre tilgang til kritisk forretningsinformasjon, forsterke kundeservicen og bedre kunne møte myndighetens krav, implementerte Winchester Business Systems tre Lotus®Domino® baserte løsninger. The Engineering Change Control Solution sørger for rask og effektiv analysering og prosessering av tekniske forespørsler, adWATCH-e hjelper Fujifilm Medical Systems å finne, distribuere, gjenopprette og administrere produktreklamasjoner, og paraFILE Document Management hjelper brukerne å finne, redigere, distribuere, gjenopprette og administrere elektroniske dokumenter (Fujifilm Medical Systems).

For å møte Fujifilm Medical Systems krav om systemsikkerhet, ble firmaets eksisterende Microsoft®Exchange system byttet ut med LotusNotes®V6. Fujifilm Medical Systems USA bruker nå Winchesters løsninger for å administrere alle FDA-regulerte dokumentbiblioteker, datateknologiske tegninger, produksjonsspesifikasjoner og kvalitetssikringsprosedyrer for sine produkter (Fujifilm Medical Systems). De nye løsningene har bidratt til at Fujifilm Medical Systems kan jobbe mer effektivt gjennom samarbeid mellom firmaets mange forretningsoperasjoner, det vil si salg, kundeservice, kvalitetssikring, tekniske operasjoner og å følge lovgivningen (Fujifilm Medical Systems).

SyBard

Vi nevnte SyBard i kapittel 2.2.4 i Litteraturreview, og det er i følge Hughes (personlig kommunikasjon, 28.april.2005) tre store brukere av denne teknologien. Den første er Ministery of Defence (MoD) i Storbritannia, som bruker SyBard/Mail, SyBard/File og SyBard/Publisher. SyBard oppnår her den påbudte sikkerheten for nivået STRENGT HEMMELIG, men dette er ikke et MLS-system da det bare har et nivå. Den andre brukeren er en forsvarsentreprenør i Storbritannia som bruker SyBard/Station for å gi designingeniørene som jobber på et HEMMELIG system, mulighet til å få tilgang til intranett og Internett på samme brukerstasjon. Den siste store brukeren av SyBard er innenriksdepartementet i Storbritannia. Det bruker en SyBard/Mail for å kunne sende e-post opp til KONFIDENSIELT nivå.

Eksisterende løsninger i Forsvaret

Forsvaret har i dag flere løsninger som støtter flere domener, eksempler på disse er partisjonert fellesnivå og tonivåløsningen. Disse gir en slags MLS med et lite spenn, men de er på langt nær gode nok til å nå målet om et NbF.

Partisjonert fellesnivå

I følge Hvinden har Forsvaret mange systemer på høyt nivå som er sammenkoblet til en viss grad, og det er dette som kalles for partisjonert fellesnivå. Dette innebærer flere domener på samme nivå og flere brukere. Partisjonert operasjonsmåte har i utgangspunktet to anvendelser. Den første er partisjonering av HEMMELIG og NATO SECRET og den andre er partisjonering av lavgradert og ugradert.

Partisjonert operasjonsmåte er en av mange mulige operasjonsmåter i grenselandet mellom fellesnivå og fullverdig multinivå. Partisjonert operasjonsmåte tilrettelegger i følge NSM (2004), for at nasjonale datasystemer skal kunne støtte et tett samarbeid med våre NATO-partnere, samtidig som sensitiv nasjonal informasjon gis nødvendig beskyttelse. Målet er at nasjonale brukere på en sikker, effektiv og brukervennlig måte skal kunne behandle både NATO-informasjon og nasjonal informasjon på en og samme arbeidsstasjon. Eksempelvis benytter internasjonale operasjoner som KFOR, SFOR og ISAF partisjonert fellesnivå på sine systemer.

Partisjonert operasjonsmåte tilrettelegger videre for at lavgraderte datasystemer skal kunne knyttes til ikke-godkjente systemer som for eksempel Internett, samtidig som lavgradert informasjon gis nødvendig beskyttelse. Et eksempel på dette er tonivåløsningen FIS/BASIS. Dette er en type MLS med lite spenn uten bruk av MLS-komponenter. Løsningen benyttes for ugradert og begrenset.

Partisjonert operasjonsmåte kjennetegnes i følge NSM (2004) ved at:

- Alle brukere har klarering for høyeste gradering som behandles
- Ikke alle brukere er autoriserte for alle graderinger
- Tilgang til data reguleres i henhold til brukeres autorisasjon og tjenestelige behov
- Systemet, inkludert applikasjoner, beskyttes mot endringer og manipulasjon fra brukere uten administrative rettigheter
- Sikkerhetsrelevante hendelser registreres slik at eventuelle sikkerhetsbrudd kan avsløres og skadeomfang og individuelt ansvar kan beregnes

Videre er hovedhensikten med partisjonert operasjonsmåte å kunne kontrollere og logge tilgang til data i henhold til autorisasjon. Partisjonert operasjonsmåte skal i følge NSM (2004) kunne:

- Hindre at brukere som et resultat av uhell, skjødesløshet eller tilsiktet handling får tilgang til data som de ikke er autoriserte for.
- Hindre at autoriserte brukere som et resultat av uhell eller skjødesløshet overfører data til ikke-autoriserte brukere.
- Fullt ut kunne spore overføringer fra høy til lav partisjon.

Fellesnivåfunksjonalitet kan i følge NSM (2004), benyttes for å implementere partisjonert operasjonsmåte. Tillitsnivået til partisjonsmekanismer skal da i størst mulig grad tilsvare CC EAL4, og hver partisjon betraktes som et fellesnivåsystem.

Personlig Brukersystem (PBS)

Hvinden nevnte meldingstjenesten i Forsvaret, PBS, som et eksempel på en MLS-løsning. Denne er i bruk i dag, og den kan sende en sensitiv melding fra en geografisk plassert PBS-stasjon til en annen.

Videre arbeid

MLS er fortsatt etterspurt i blant annet forsvarsmiljøer, og vi vet at både NATO og SAP har arbeidsgrupper som jobber med å finne MLS-løsninger. Forsvarsleverandører og andre store firmaer jobber stadig med videre utvikling av allerede eksisterende og nye systemer for MLS. For SAP finnes DEIG (Defence Interest Group) som ser på MLS-versjoner av SAP. SAP kan

realisere mye av den ønskede funksjonaliteten, men i følge Ølnes "*vil det være umulig å sertifisere SAP til EAL4 eller lignende*".

Troen på MLS

De klassiske strategiene medførte at MLS-produktene mislyktes på flere måter. I følge Smith (2005) mislyktes den amerikanske statens promotering av produktevalueringer da leverandører fant at MLS-mulighetene ikke ville øke produktsalget betydelig. Konseptet med å sette inn et påvist sikkert system mislyktes to ganger; først da leverandørene fant ut hvor kostbare og uvisse evalueringene kunne bli, og andre gang da sikkerhetseksperter avslørte hvor vanskelig problemet med skjulte kanaler kunne bli. Til slutt dovnet de få MLS-produktene på veg inn i markedet bort, da sluttbrukerne innså hvor snevert produktene løste deres sikkerhetsproblemer og delingsproblemer.

På tross av feil og frustrasjoner som har forfulgt utviklingen av MLS-produkter siden starten, etterlyser sluttbrukere fortsatt MLS-muligheter. I forsvarssammenheng trengs informasjonsdeling på flere sikkerhetsnivåer. De fleste løser problemet ved å arbeide på flernivådata på fellesnivå operasjonsmåte, og å behandle nedgraderingsproblemer hver for seg. De viktigste suksessene i MLS i dag er i følge Smith (2005) basert på guard og tiltrodde serverprodukter.

I forbindelse med intervjurundene blant ansatte i Forsvaret, benyttet vi anledningen til å finne ut hvilke tanker de ansatte hadde vedrørende innføring av MLS i forsvarssammenheng. Blant det operative personellet var det store sprik i synspunkter på om og eventuelt når, et MLS-system kan bli en realitet i Forsvaret. Enkelte mente faktisk at et MLS-system ville komme innen fem år.

Ingen av de ikke-operative intervjuobjektene ville si noe om når Forsvaret kan ta i bruk MLS. De mente at de ikke hadde forutsetninger for å mene noe om dette. Det var imidlertid ingen som hadde tro på en MLS-løsning i nær fremtid. Nakstad sa at han hadde tro på en løsning med ulike roller, der man kan logge på flere steder flere ganger, men heller ikke han hadde tro på noen fullverdig MLS-løsning.

Hvinden ga uttrykk for at det største hinderet for en innføring av MLS i forsvarssammenheng, er mangel på funksjonalitet, fleksibilitet, brukeraksept, robusthet, ajourhet, samt pris i full/klassisk MLS. Produktet er etter hans mening ikke kommersialisert nok, og det finnes dessuten ikke MLS på Windows, kun på Linux.

Det er altså svært få som har tro på at et MLS-system noensinne vil bli innført. Mange av de som jobber i Program Golf og FLO/IKT har mer tro på løsninger med delvise MLS-egenskaper.

Fremtidsutsikter

For mange kommersielle virksomheter gir ikke BLP-kontrollene i følge Anderson (2001) nok beskyttelsesgevinst i forhold til de høye utviklingskostnadene. Dessuten er produkter som er godt kjent i markedet ofte bedre på grunn av utviklingen som kommer som et resultat av store mengder tilbakemeldinger fra brukerne. Kanskje den virkelige fremtiden for MLS-systemer ikke er innenfor konfidensialitet, men integritet. Mange nåværende systemer implementerer varianter av Biba-modellen, selv om mange av designerne ikke har hørt om ordet Biba.

I følge Anderson (2001) har forskerne nå begynt å lage modeller med både konfidensialitet og integritet for å se på samhandlingen mellom disse, og hvordan de kan brukes i forbindelse med for eksempel smartkort. En annet aktuelt emne er hvordan MAC-modeller kan skaffe sanntids ytelsesgarantier for å hjelpe til med å forebygge servicebenektelsesangrep.

Alternativ til MLS

”*Hvis ikke markedet frembringer MLS-produkter med tilstrekkelig tillit for bruk i et flernivås NbF, må ambisjonsnivået for NbF trolig reduseres noe. En realistisk mulighet er da å videreføre dagens arkitektur med to separate fellesnivåsystemer. Dersom det er behov for utveksling av data mellom de to plattformene, kan dette ivaretas gjennom spesielle rutiner eller utvikling av spesielle filtermekanismer med høy tillit og spesialisert funksjonalitet.*” (Pedersen et al., 2004).

MSL

Vi forhørte oss blant intervjuobjektene om hvilke tanker de hadde om MLS som en del av Forsvaret i fremtiden. Noe overraskende stilte alle seg svært tvilende til om en fullverdig MLS-løsning noen gang vil bli en realitet. Flere nevnte MSL som mulige løsninger. Ølnes uttrykte blant annet at: ”*I Golf FP2 skisserte vi integrasjonsstrategier basert på Web Services og sikkerhetsgatewayer. Poenget er en sterk soneinndeling og sterk kontroll på trafikk mellom soner (enten disse er på forskjellige graderingsnivåer eller innen samme graderingsnivå). Strategien er da ikke store MLS-systemer, men separate systemer og ”MLS-integrasjonsløsninger”. I noen dokumenter er dette omtalt som MSL (Multi System Level).*”

Videre uttalte han at: ”*Jeg/vi i FP2 har liten tro på at store systemer på noen praktisk måte kan være MLS (bl.a. pga. sertifiseringer). Derfor separate systemer og systemintegrasjon, der deler av integrasjonsløsningene (sikkerhetsgatewayer) må være MLS. Dette stiller også krav til intern sikkerhet i hver sone/system, men i hovedsak kan disse kravene være iht. det som gjelder for det aktuelle graderingsnivået.*”

5.2.13 Oppsummering

Sammenlikning av egenskapene til de ulike modellene og strategiene

Tabell 5: Sammenlikning av modell egenskaper.

Egenskapene		Modeller							
		BLP	BLP Rev.	MMS	SNet	Vijay	Atluri	NRL	DBSy
Motivasjon	Modellen er laget for et spesielt system/applikasjon			X	X				
	Laget for å veilede konstruksjonen av fremtidige systemer	X	X			X	X	X	X
Syn på sikkerhet	Modellerer tilgang til objekter uten å ta hensyn til innhold	X		X		X			
	Modellerer flyt av informasjon mellom objekter		X		X	X	X	X	X
Annet	Systemer som er basert på modellen har blitt implementert	X	X	X	X				
	Modellen er formell	X	X	X	X	X	X		
	Modellen er primært laget for forsvarsbruk	X		X				X	X

BLP = Bell & La Padula (1973), BLP rev. = Feiertag et al. (1977), MMS = Landwehr (1984), SNet = Glasgow & MacEwen (1987), Vijay = Varadharajan (1990), Atluri= Atluri et al.(1997), NRL = Kang et al. (1999), DBSy = Robinson (2001); Hughes (2002); Warrener (2003).

Motivasjon

Det er i hovedsak to motivasjoner som styrer konstruksjonen av en formell modell. Det er enten å lage en modell for et spesifikt system, eller å lage en generell modell.

Det er slik at det meste av arbeidet med MLS har vært og er fortsatt, i stor grad dominert av det amerikanske forsvaret. Som vi nevnte i kapittel 5.2.2, ble det et kraftig kutt i USAs og andre lands forsvarsbudsjetter etter slutten av den kalde krigen. Dette medførte mindre ressurser til forskning og utvikling innen MLS, noe som igjen førte til en vesentlig endring vedrørende motivasjonen. Det er sannsynligvis billigere og enklere å lage en modell for et spesifikt system enn å lage en generell modell. En vet da gjerne konkret hva modellen skal brukes til og kan forholdsvis enkelt skreddersy modellen til systemet. Mindre ressurser har ført til at det i de siste årene har blitt utviklet svært få generelle modeller innen MLS.

Syn på sikkerhet

Modellene, strategien og metoden for MLS kan i hovedsak deles inn i to sikkerhetsgrupper; de som er ute etter å kontrollere tilgangen til bestemte objekter (BLP og MMS), og de som er opptatt av informasjonsflyten mellom objektene (BLP rev., SNet, Atluri, NRL og DBSy). Vijays modell håndhever begge synene. Hvilket syn og hvilken modell som bør velges avhenger helt av applikasjonen og hvordan nettverket vil fungere. Vi ser en klar sammenheng mellom synet på sikkerhet og alderen til modellene. De eldste modellene har ofte tilgangskontroll på objektene, mye på grunn av at systemene tidligere var flerbrukersystemer og ikke nettverksbaserte systemer. De nyere modellene har ofte informasjonsflyt, og det virker som at informasjonsflytmodeller er det som regjerer i dagens MLS-miljø.

Annet

Seks av åtte strategier og teorier er formelle modeller. De formelle modellene er matematisk bevist, og regnes som sikre i forhold til det de er bygget til. Dette er et krav for å få til et fullverdig MLS-system.

Vi kan med sikkerhet si at fire av modellene har blitt implementert i systemer. Vi er usikre på hvorvidt de øvrige modellene har blitt implementert. Vi har ikke funnet noe som tyder på dette, men det finnes svært lite publisert informasjon rundt dette.

Av de åtte modellene vi har gått igjennom, er det bare fire som vi med sikkerhet kan si at er laget primært for en militær setting. Vi er imidlertid av den oppfatning at de øvrige modellene kan endres, slik at de også kan tilrettelegges for en militær setting. En slik endring vil selvfølgelig koste en del penger, men er kanskje en rimeligere løsning enn å starte helt på nytt.

MLS-systemer og fremtiden

Tabell 6: Oppsummering av MLS–systemene.

Navn	I bruk i dag?	Gir fullverdig MLS?	Evalueringsnivå
PBS	*Ja.*	*Nei, bare meldingstjeneste.*	-
Partisjonert fellesnivå	*Ja.*	*Nei, bare delvis.*	-
Sun Trusted Solaris v1.1	*Mulig, men den produseres ikke lengre.*	*Er et operativsystem.*	*TCSEC – B1*
IBM – Fujifilm Medical Systems	*Ja.*	*Ja, for et firma, men neppe for en militær organisasjon.*	-
RAF's LITS	*Nei.*	*Nei, bare for et lite miljø.*	-
SyBard	*Ja, flere tunge Forsvarsselskaper i UK bruker denne teknologien.*	*Nei, fordi tiltroen til systemet ikke er høy nok til en militær organisasjon*	*Skal testes i CC for EAL4 tiltro.*
CMW	*Nei*	*Nei, gir bare muligheten til å se forskjellige sensitive data på en og samme PC.*	*Det finnes flere CMW systemer, så da er det naturlig med forskjellige evalueringer.*
AT&T's System V/MLS	*Vet ikke.*	*Er et operativsystem.*	-

"-" = vi har ikke funnet noe evaluering

Det har i løpet av historien vært mange forsøk på å oppnå MLS. Det finnes eldre løsninger som Oracle og Sun Trusted Solaris, og nyere løsninger som SyBard og IBM. Det har også vært flere forsøk på å lage MLS-logistikksystemer, men de fleste har endt i svært dyre fiaskoer.

Det norske forsvaret bruker som kjent partisjonert fellesnivå, som en slags MLS-løsning i dag. Partisjonert operasjonsmåte er en av mange mulige operasjonsmåter i grenselandet mellom fellesnivå og fullverdig multinivå. Forsvaret bruker også meldingstjenesten PBS, der en kan sende opp til STRENGT HEMMELIGE meldinger fra en PBS-stasjon til en annen.

MLS er fortsatt etterspurt i forsvarsmiljøer, og det jobbes fortsatt aktivt med dette blant annet i SAP og i NATO. SAP har opprettet en egen gruppe, DEIG, som skal se på muligheten å implementere MLS i SAP. Resultatene fra intervjuene viste at det var store sprik blant det operative personellet, vedrørende synspunkter på om og eventuelt når, et MLS-system kan bli en realitet i Forsvaret. Enkelte mente at MLS kunne bli en realitet innen fem år, mens andre trodde at det aldri ville bli en realitet. Blant de ikke-operative intervjuobjektene var det ingen som ville forutsi når et eventuelt MLS-system ville komme. I fremtiden kan det kanskje komme systemer som ikke er innenfor konfidensialitet, men integritet, siden den

kommersielle delen av samfunnet heller vil ha dette. Det er også nevnt at fremtidens modeller vil innlemme begge disse i en og samme modell. Vi har funnet svært få alternativer til MLS, men flere av våre intervjuobjekter nevnte MSL som en mulighet.

5.3 Delproblem 3: Konsekvenser ved innføring av Multilevel Security

Vi skal utrede konsekvensene av innføringen av et system som sammenkobler informasjon med ulik sikkerhetsgradering.

5.3.1 Bakgrunn

Forsvaret skal utvikles i retning av et NbF der systemunderstøttelsen i størst mulig grad er lik i fred, krise og krig, i og utenfor Norge. Konseptet NbF baserer seg på informasjonsoverlegenhet og utnyttelsen av en slik overlegenhet for å oppnå økt felles situasjonsbevissthet, økt tempo i operasjonene, økt stridsevne, økt overlevelse og selvsynkronisering (Pedersen et al., 2004).

Noen av de muligheter og effekter som antas å kunne oppnås gjennom nettverksbaserte konsepter, er i følge Pedersen et al. (2004) økt deling av informasjon og kunnskap, bedre samarbeid, bedre og enklere koordinering og synkronisering, samt distribuert og virtuell organisering.

Vi har på bakgrunn av to kvalitative undersøkelser, henholdsvis blant operativt og ikke-operativt personell i Forsvaret, redegjort for mulige konsekvenser ved en eventuell innføring av MLS i Forsvaret.

5.3.2 Metode

I første omgang har vi gjort undersøkelser blant operativt personell i Forsvaret. Vi har i denne forbindelse undersøkt brukervennligheten på nåværende systemer for gradert informasjonsflyt. Videre har vi klarlagt hvilke synspunkter det operative personellet har vedrørende innføring av MLS. Dette dreier seg om hvorvidt et MLS-system kan forenkle eller effektivisere arbeidssituasjonen.

Dernest har vi utført undersøkelser blant ansatte innen sikkerhet og IKT, vedrørende hvilke konsekvenser en innføring av MLS, vil kunne medføre for Forsvaret. Dette dreier seg om aspekter innen sikkerhet, brukervennlighet, informasjonsflyt, lagring av data, opplæring og det økonomiske aspektet.

Intervjuene med den førstnevnte gruppen ga oss resultater vedrørende brukervennlighet og lagring av data på nåværende systemer i forhold til på et tenkt MLS-system. Resultatene fra den andre gruppen omhandlet hovedsakelig resultater i forhold til syn på sikkerhet.

Resultatene fra begge undersøkelsene ble behandlet felles og systematisert etter ulike konsekvenser.

5.3.3 Resultater

Hovedsynspunktene blant intervjuobjektene er at en eventuell innføring av MLS vil være positivt både for Forsvaret som organisasjon og for den enkelte arbeidstaker. Flertallet av intervjuobjektene både blant operativt og ikke-operativt personell, ser flere fordeler enn ulemper med innføring av MLS i Forsvaret.

Konsekvens 1: Sikkerhet

For oss kan det virke som at sikkerheten vil være det mest kritiske ved en eventuell innføring av MLS. Over halvparten av de spurte ga uttrykk for at et MLS-system vil kreve nøye merking av data og sette store krav til brukerne. Når det gjelder lagring av data, så er det slik at dersom en person er logget inn på HEMMELIG, blir også informasjonen HEMMELIG. Det er ikke mulig for en bruker å være logget på to nivåer samtidig, og det vil derfor være spesielt viktig med grundig opplæring vedrørende riktig merking av data på et MLS-system. Bruk av MLS-systemer krever god kontroll med autorisasjon til brukerne, og det er viktig å argumentere for hvorfor den enkelte trenger tilgang. Slik vi har forstått det, er det forholdsvis enkelt å få tilgang med dagens ordning. Liberg understrekte at tjenestemessige behov bør være klare og styrende, og sa videre at: ”*Personellsikkerheten blir enda viktigere med MLS, spesielt med tanke på hvem som får tilgang til hva.”*. Nakstad uttrykte at: *”Rolletildelinger og personlig ansvar; her kreves det en stor oppvask. Hvis ikke, vil sikkerheten bli dårligere”*.

Basert på intervjuene er de fleste positive til et MLS-system i Forsvaret, dersom gode nok løsninger blir tilgjengelige og lar seg gjennomføre. Det de stiller seg kritiske til, er forholdene rundt sikkerheten, blant annet lekkasje av informasjon. Liberg mente at i en krigssituasjon, vil det være fare for at fienden kan komme seg inn på systemet og få tak i sensitiv informasjon. Men han mente også at: *”Informasjonsoverlegenhet overgår mulig lekkasje av informasjon”*.

Det operative personellet hadde delte meninger om hvorvidt et MLS-system vil være mindre sikkert enn dagens systemer. Person A og D mente at et eventuelt MLS-system vil stille betydelig større krav til brukerne. A mente at: *”Det vil kreve at hver enkelt bruker er bevisst på hvilken gradering som er gjeldende, for å forhindre at uvedkommende får adgang til informasjon”*. Med andre ord mente person A at sikkerheten kan bli dårligere med MLS. Person C mente at sikkerheten ikke vil bli dårligere, med det forbeholdet om at datamaskinene kvalitetssikrer det brukerne gjør, slik at sensitiv informasjon ikke kommer på avveie.

Konsekvens 2: Brukervennlighet

Fujifilm Medical Systems, som vi presenterte i kapittel 5.2.12, har opplevd en mengde positive erfaringer med sitt MLS-system. Firmaet har blitt mer effektivt og oversiktelig, de

ansatte opplever bedre brukervennlighet, firmaet når fortere ut til kundene og kundeservicen har blitt merkbart bedre (Fujifilm Medical Systems).
Når det gjelder personene vi intervjuet, så mente Ølnes at effekten for brukerne ikke ville være særlig stor ved en eventuell innføring av MLS. Videre sa han at hvis brukereffekten ble stor, ville sikkerheten i systemet neppe være god nok.

De fleste av intervjuobjektene i vår undersøkelse, bytter sikkerhetsnivå minst ti ganger daglig og arbeider på tre forskjellige brukerstasjoner. Vedrørende brukervennligheten på dagens systemer, mente de fleste at denne er lite god. Person A svarte: ”*Det medfører unødvendig mye ekstraarbeid at forskjellige graderinger ikke kan benyttes på forskjellige systemer. For å utføre primærfunksjon er det nødvendig å utveksle informasjon mellom systemer, og det tar uforholdsmessig mye ressurser å gjøre dette.*” Person C underbygde As mening med å si: ”*Svært lite brukervennlig, da alt som skal til et høyere graderingsnivå må tas ut på memostick, og alt som skal til et lavere nivå må brennes ut på CD. Veldig tidkrevende.*” Det er med andre ord stor missnøye med dagens løsning der en benytter flere brukerstasjoner.

Størstedelen av de ikke-operative intervjuobjektene ga uttrykk for at et MLS-system sannsynligvis vil forenkle situasjonen for alle. Videre mente de at det operative personellet sannsynligvis vil merke de største endringene. Dette på grunn av at de vil få tilgang til informasjon hvor som helst og når som helst, fra hvilken som helst datamaskin. Nyquist bemerket imidlertid at en MLS-implementering kan medføre et system som er vanskeligere å administrere enn dagens systemer.

Det operative personellet hadde delte meninger om hvordan det er å arbeide på nåværende systemer. Helhetsinntrykket er likevel at de fleste oppfatter dagens ordning som tungvind og tidkrevende. Person C mente at: *”Det hadde jo vært greit å forholde seg til et system, i stedet for fire. Jeg ville spart mye tid på det, og ikke minst: ”Hvor var det nå jeg hadde de filene?”.* Det å få tilgang til all informasjon fra et sted, hvor som helst og når som helst, er trolig den største fordelen med et MLS-system. Brukerne vil få mer tid til å utføre sine oppgaver mer effektivt. Til eksempel uttrykte person A: *”Jeg vil med et slikt system kunne konsentrere meg om primærfunksjonene i stedet for å bruke ressurser på å skifte mellom ulike nett.”*.

Konsekvens 3: Informasjonsflyt

I Fujifilm Medical Systems har informasjonsflyten bedret seg betraktelig etter at de implementerte MLS-systemet fra IBM (Fujifilm Medical Systems). Dette har blant annet ført til at de ansatte jobber mer effektivt, og at samarbeidet mellom firmaets mange forretningsoperasjoner har blitt betraktelig bedre.

Målsettingen med NbF er informasjonsoverlegenhet i forhold til andre nasjoner. Vi tror at det å innføre et MLS-system, er middelet som må til for å få til dette. MLS vil etter vår mening gi

betydelig bedre informasjonsflyt, både mellom graderingsdomener og mellom enheter i organisasjonen.

De fleste av de ikke-operative intervjuobjektene antok også at MLS vil gi bedre informasjonsflyt og bidra til å skaffe Forsvaret informasjonsoverlegenhet. Nyquist på sin side uttalte at: ” *Hverdagen for brukere på alle nivåer (saksbehandler, leder, controller etc.) og innen alle funksjonsområder vil få bedre systemstøtte for sine arbeidsprosesser. Kjempefordel med flere graderinger på samme system.”*. Hvinden nevnte et eksempel med at en beltevogn mistet beltet. Han så da for seg at et MLS-nettverk ville kunne gjøre det mulig å bestille beltet direkte av logistikkavdelingen, uten noe form for ekstra kommunikasjon. Med et slikt system vil en unngå duplekse oppkjøp, samtidig som at lagerdata og logistikkdata blir lettere å holde orden på. Med andre ord så vil informasjonsflyten mellom leddene bli betraktelig forbedret.

Blant det operative personellet mente person A at: *”Et felles system for ulike graderingsnivåer hadde gjort informasjonsflyten enklere, for ikke å si mulig. Dette gjelder spesielt mellom norske systemer og NATO-systemer.”* A sier her at informasjonsflyten ville blitt mulig å utføre, noe som kanskje ikke er mulig i dag. I så fall indikerer person A at dagens informasjonsflyt er altfor tungvindt.

Konsekvens 4: Lagring av data

Et MLS-system vil trolig være økonomisk besparende rent lagringsmessig. Slik situasjonen er i dag er mye av dataene lagret flere steder. Videre er det ofte forskjellig informasjon i ulike systemer vedrørende materiell og annet. Liberg spør seg selv: *”Hvilken informasjon skal man stole på i en krigssituasjon? Er informasjonskvaliteten høyest på HEMMELIG eller BEGRENSET?”*. MLS kan absolutt sette slike problemer til livs.

Person A i brukerundersøkelsen mente blant annet at det var 70 – 90 % dupleks informasjon på nettene med HEMMELIG og NATO SECRET informasjon. A mente videre at problemet ikke var at det var for høy gradering på informasjonen, men at en altfor ofte bruker nasjonale graderinger på informasjon som like gjerne kan gis NATO-gradering. De øvrige brukerne, det vil si person B, C og D, mente at det var 10 – 30 % dupleksinformasjon på de ulike nettene. Det kom også frem at flertallet mente at 0 – 30 % av informasjon vil bli nedgradert til BEGRENSET hvis innføring av MLS blir en realitet. På de HEMMELIGE nettene var meningene delte om hvorvidt det var 40-60 % eller 0-30 % av informasjonen, som kunne bli nedgradert. Person A hadde en annen løsning på problematikken: *” Jeg mener at bruken av nasjonale graderinger brukes i alt for stor grad. Det er innlysende at noe må holdes på nasjonalt nivå, men store deler av den informasjonen som i dag graderes nasjonalt etter min oppfatning, kan gis en NATO-gradering. Dette vil gjøre forholdene bedre, spesielt i multinasjonale miljøer.”* Dette kan kanskje løse problematikken med at mye HEMMELIG informasjon ligger på to nett, men det vil ikke løse nedgraderingsproblematikken.

Konsekvens 5: Opplæring

Vi har nevnt tidligere at en eventuell innføring av MLS vil kreve større kontroll med hensyn til tildeling av roller og autorisasjon av brukere. Samtidig vil det sette høye krav til brukerne med tanke på merking av data. For at dette skal fungere på en tilfredsstillende måte, mener vi at Forsvaret må sette inn store ressurser til opplæring blant brukerne.

Hvinden nevnte at hvis en har et ideelt produkt og opplæring blant brukene, så vil MLS bli mulig. Med andre ord så trenger en ikke bare riktig teknologi, men også opplæring av brukerne. Opplæringsprosessen er noe som det må innarbeides gode rutiner for, slik at nytt personell får opplæring umiddelbart etter at de har begynt. Videre vil det etter vår mening være svært viktig med tett oppfølging i starten, og deretter oppfriskningskurs med jevne mellomrom.

Konsekvens 6: Det økonomiske aspektet

Et annet moment ved en eventuell MLS-innføring, er det økonomiske aspektet. Flere av intervjuobjektene ga uttrykk for at en innføring av et slikt system vil bli svært kostnadskrevende, både med tanke på utviklingen av et MLS-system og selve implementeringen.

Liberg ga uttrykk for at MLS i Forsvarssammenheng krever et samspill mellom leverandør (for eksempel IBM), kunde (for eksempel Program Golf) og NSM, der alle blir enige om hva man ønsker å oppnå. Han sa videre at kostnadene må deles mellom interessentene og at ”*Det store spørsmålet er om markedet er stort nok til at en leverandør vil koste utviklingen av et MLS-system alene. Dette er tvilsomt, og må trolig baseres på kostnadsdeling mellom flere Nato-land*.”

Blant det operative personellet utdypet person A med at: ”*Dette er noe som krever evne, vilje og ikke minst penger. Jeg tror at evnen er der, til tider viljen – i hvert fall hos de som jobber i operative miljøer, men at det ikke kommer til å bli avsatt nok midler til å dekke inn økonomien. Noen vil kanskje se et slikt system innenfor sitt begrensede kontorlandskap, mens de som har størst behov, ikke vil se noe til systemet. Tviler sterkt på at det vil bli utplassert om lag hundre klienter i Kabul. Om systemet skal ha noen hensikt, er dette noe alle må ha tilgang til.*” Det operative personellet hadde delte meninger om når et MLS-system vil realiseres i Forsvaret. Person A og D mente at det aldri vil bli en realitet. B på sin side, antok om to til fem år, mens C mente at MLS ville innføres innen 6-10 år.

Det vil uten tvil være kostnadskrevende å innføre et MLS-system i Forsvaret. Flere av intervjuobjektene mente imidlertid at MLS på sikt kan bli både kostnadsbesparende og personellbesparende i forbindelse med drift.

Personlig tror vi i likhet med flere av intervjuobjektene fra Golf og FLO/IKT, at en innføring av et MLS-system vil kreve enorme implementerings- og opplæringskostnader. På den annen side tror vi at det vil være kostnadssparende på sikt. Forsvaret vil kunne redusere antall brukerstasjoner rundt om i organisasjonen, og de ansatte vil bruke mindre tid på administrere gradert informasjon. Slik som det er i dag, skifter det operative personellet ofte mellom tre og flere brukerstasjoner daglig, og skifter mellom sikkerhetsnivåene et tosifret antall ganger på en dag.

5.3.4 Oppsummering

En av de største utfordringene ved en eventuell innføring av et MLS-system, er å opprettholde sikkerheten på et tilfredsstillende nivå. Dette gjelder særlig i forhold til rolletildelinger og personlig ansvar. Vi mener at sikkerheten i stor grad kan ivaretas med god opplæring og oppfølging av brukerne.

Vi har fått inntrykk av at dagens løsning oppfattes som tungvind og tidkrevende for det operative personellet, og at de i aller høyeste grad ser nytten av å innføre et MLS-system. De fleste brukerne mente at et MLS-system vil gjøre hverdagen deres enklere. Flertallet ga uttrykk for at et slikt system sannsynligvis vil bidra til at de kan bruke mer tid på sine primærfunksjoner, i stedet for å bruke tid på skifte mellom systemer. De mente også at brukerterskelen på et MLS-system vil bli lavere enn på dagens systemer. Brukerne poengterte videre at en innføring av et slikt system vil kreve mer av dem som brukere, siden det ikke lenger vil være en fysisk sperring mellom graderingsnivåene.

Det er klart at det å innføre MLS vil medføre store kostnader i forbindelse med investering og implementering. Vi tror imidlertid at det på sikt kan være kostnadsbesparende. Videre vil det uten tvil gjøre hverdagen betydelig enklere for det personellet som jobber på ulikt graderte nett. For det første vil de kunne slippe hyppig skifting mellom brukerstasjoner, og det vil trolig bli mindre dupleks lagring av data. Sistnevnte vil som nevnt tidligere, fjerne problematikken med at en ikke vet hvilken informasjon en skal stole på.

6 Drøfting

6.1 Innledning

Drøftingen er basert på resultatene fra de tre første delproblemene. Først har vi vurdert gjeldende krav for sikkerhet og evaluering. Deretter har vi drøftet teorier, strategier og systemer innen MLS, og hvilke konsekvenser Forsvaret kan oppleve ved en MLS-innføring. Til slutt i kapittelet har vi drøftet oppgavens validitet, med hensyn til metode og resultater.

6.2 Gjeldende krav

Resultatene viser hvilke krav som må tilfredstilles for å kunne innføre et fullverdig MLS-system i Forsvaret, og dermed oppnå målet om et NbF. Funnene tyder på at både gjeldende sikkerhetskrav og evalueringskrav kan være til hinder for en slik innføring.

6.2.1 Sikkerhetskrav

De største hindringene er trolig Sikkerhetsloven (2001) og NATO-policyen som setter grenser for og stiller krav til, sammenkoblinger av systemer med forskjellige graderingsnivåer. *Hvert sammenkoblet system skal ha en beskyttelse mot andre informasjonssystemer, og sikkerheten i det enkelte system skal bare baseres på mekanismer i vedkommende system"* (Forskrift om informasjonssikkerhet, 2001, § 5-4). Sikkerhetsloven forbyr kort sagt at HEMMELIGE systemer kobles mot Internett.

I Norge er det som kjent NSM som håndhever og tolker Sikkerhetsloven. NSM må rette seg etter kravene som er gitt i NATO-policyen, og kan derfor ikke uten videre endre gjeldene krav. Kravene i Sikkerhetsloven og i NATOs lovverk er forholdsvis strenge sammenliknet med andre sikkerhetskrav. Hovedgrunnen til dette er at Forsvaret har mye høyt gradert informasjon. I verste fall kan informasjon som kommer på avveie, medføre risiko for rikets sikkerhet.

De strenge kravene er etter vår mening med på å hindre utviklingen av ny MLS-teknologi, nye tankeganger, og ikke minst, viljen til å utføre et omfattende MLS-prosjekt i forsvarssammenheng. Den strenge linjen er med på å vanskeliggjøre samarbeid med utviklingsmiljøer. Dagens krav gjør at flere utviklere og leverandører ikke ser noen hensikt i å jobbe med en MLS-løsning for Forsvaret. De vil uansett ikke få godkjent en fullverdig MLS-løsning på grunn av regelverket.

Det er tydelig at gjeldende sikkerhetskrav hindrer målet om et NbF, som krever en fullverdig MLS-løsning. Forsvaret kan velge å la dagens krav være som de er. Dette vil neppe føre noen veg i forhold til MLS. Et annet og ut ifra vårt synspunkt, bedre alternativ, er å gå aktivt inn for å gjøre noe med situasjonen. Sannsynligvis er det flere nasjoner i NATO som ønsker å endre nåværende sikkerhetskrav. Det kan være hensiktsmessig for Norge å alliere seg med disse, og

sammen jobbe aktivt med en kravendring opp imot NATO. Etter vårt syn, er det viktig at Norge deltar i en slik prosess, for ikke å bli hengende etter i utviklingen.

En løsning som kan godkjennes med dagens regelverk, er å definere BEGRENSET som laveste nivå, og la være å koble nettverket til Internett. Dette vil minske funksjonaliteten; blant annet vil en miste muligheten til å koble seg til nettverket hvor som helst. Systemet vil videre være begrenset til å gjelde kun for Forsvaret, og kan ikke betegnes som et fullverdig MLS-system. Et slikt lukket system er mindre utsatt for inntrengere og dermed sikrere enn et fullverdig MLS-system. Det kan likevel være utro tjenere i organisasjonen; dette har man aldri garanti mot. Selv de mest tiltrodde personer har lekket informasjon gjennom historien.

Ovenstående løsning kan etter vår mening tilfredsstille gjeldene sikkerhetskrav. Følgelig er den ingen fullverdig MLS-løsning, men et mulig alternativ inntil kravene eventuelt endres. Dersom kravene hadde blitt senket, ville Forsvaret trolig hatt mulighet til å innføre et MLS-system i nær fremtid. Per i dag finnes det ikke god nok teknologi til å bygge et fullverdig MLS-system, men en endring i gjeldende krav ville trolig gjøre det hele mer interessant for utviklere og leverandører.

6.3 Evalueringskriterier

Per i dag er det evalueringskriteriene i CC som er gjeldende. Basert på intervjuer og kontakt med annet fagpersonell, har vi fått inntrykk av at flere anser disse kriteriene som altfor strenge. Nyquist var blant de som påpekte dette. Han fikk støtte for sitt syn både av Wiseman og Hughes, begge fra QinetiQ.

"S*ystem designs requiring more than Common Criteria EAL4 assurance should be avoided, because higher assurance is only found in a few specialised products."* (Pomeroy & Wiseman, 1998, s. 3). Med dagens høye evalueringskrav, er vi langt på veg enige med Pomeroy og Wiseman. Det er svært vanskelig å få godkjent et system med høy tiltro. For det første finnes det kun et fåtall produkter som har høy nok sertifisering til å kunne brukes. For det andre er sertifisering av nye produkter og systemer svært kostbart. Og jo høyere sertifisering en ønsker, dess dyrere blir det. Utvikling av et system med høy tiltro, slik som et MLS-system, innebærer altså enorme kostnader.

Tiden er kanskje inne for å gjennomgå behovene og kravene på nytt. En endring av CC er noe som kan ta lang tid, både på grunn av at det ikke er en felles oppfatning i evalueringsmiljøet, og fordi det er en lang prosess. Et sted må man imidlertid begynne. Slik vi ser det, er tiden inne for å utarbeide nye evalueringskriterier beregnet på dagens teknologi og tankegang. Kriterier tilpasset moderne systemer vil sannsynligvis forenkle selve evalueringen. I tillegg vil sannsynligvis kostnadene bli vesentlig lavere.

For oss virker det som at CC sammen med gjeldende sikkerhetskrav, bremser prosessen med å oppnå MLS. Per i dag er det forholdsvis dyrt å evaluere systemene i CC. Videre er det svært kostbart å utvikle systemer basert på de gjeldende kravene.

6.4 Teorier og strategier innen Multilevel Security

Vedrørende teorier og strategier innen MLS, er spørsmålet om noen av dem kan brukes som en grunnleggende arkitektur for et fremtidig MLS-system. Med gjeldende CC, må en formell modell ligge til grunn for et stort MLS-system, som det Forsvaret er ute etter.

Tabell 7: Oversikt over de modellene, strategien og metoden vi har valgt.

Navn	År	Sikkerhetspolitikkmodell	Arbeidsflytmodell	Strategi	Metode
BLP	1973	X			
Rev.BLP	1977	X			
MMS	1984	X			
SNet	1987	X			
Vijay	1990	X	X		
Atluri	1997		X		
NRL	1999			X	
DBSy	2000				X

BLP = Bell & La Padula (1973), BLP rev. = Feiertag et al. (1977), MMS = Landwehr (1984), SNet = Glasgow & MacEwen (1987), Vijay = Varadharajan (1990), Atluri= Atluri et al.(1997), NRL = Kang et al. (1999), DBSy = Robinson (2001); Hughes (2002); Warrener (2003).

Det har blitt publisert svært lite informasjon om MLS etter 1990. Flere av modellene vi har valgt ut, er derfor gamle, og kan være vanskelige å bruke i forhold til dagens teknologi. Teoriene, strategien og metoden gir et innblikk i hva som er gjort tidligere. De viser hva som har fungert og hva som ikke har fungert, og hvordan tankegangen har utviklet seg gjennom årene. Dette gir en grei innføring i hvordan MLS har forløpt siden starten, og kan være nyttig informasjon i forbindelse med utvikling av en ny formell modell.

BLP-modellen er trolig den best kjente modellen innen MLS. Vi mener imidlertid at denne er gammel og utdatert; med andre ord ikke noe å satse på. Tankegangen er gammeldags og modellen har dessuten flere svakheter. Den største svakheten med BLP-modellen er etter vår mening at den ikke støtter nedgradering av informasjon. Nedgradering av informasjon er blant de viktigste egenskapene for et MLS-system. Uten en nedgraderingsfunksjon vil det hope seg opp mye informasjon. Dette kan for eksempel være informasjon som er merket HEMMELIG, men som egentlig er BEGRENSET. Likevel var BLP-modellen ganske nytenkende i sin tid, med stjerneegenskapen som effektivt kunne beskytte datasystemer fra angrep som kunne føre til informasjonslekkasje. Den største styrken til modellen var at den gjennom stjerneegenskapen og den enkle sikkerhetsegenskapen, gjorde det mulig for andre å teste ut ulike teoremer. Dette er hovedgrunnen til at den betegnes som den klassiske MLS-modellen. De andre BLP-baserte modellene, som Feiertag et al. (1977) og Landwehr (1984) sine modeller, arvet mange av egenskapene til den opprinnelige BLP-modellen.

Arbeidsflytmodellene viser hvordan en kan få til arbeidsflyter mellom forskjellige nivåer. Rene arbeidsflytmodeller har som kjent ikke tilgangskontroll. Varadharajans (1990) modell har både arbeidsflyt og tilgangskontroll, og betegnes derfor som en kombinasjonsmodell. Den har sikkerhetsegenskaper fra BLP og MMS, og samtidig arbeidsflyter innlemmet i politikken. I arbeidsflytmodeller er det ikke snakk om hvordan en skal merke et objekt, men hvordan en skal merke en arbeidsflyt. Atluri et al. (1997) viser hvordan dette gjøres. For å få laget et fullverdig MLS-system, må MLS-arbeidsflytmodellen være formell og ha en underliggende, godkjent MLS-arkitektur. I tillegg kreves tiltrodde mekanismer som kan gi tilstrekkelig sikkerhet.

Kang et al. (1999) har gjort et forsøk på å få til en MLS-arbeidsflyt. Det ligger imidlertid ikke noen formell modell bak strategien, hvilket hindrer en fullverdig MLS-løsning. Dette tyder på at det er et behov for en ny og formell modell. En ny modell vil trolig være til stor hjelp i flere sammenhenger, blant annet for SAP DEIG. De jobber med en løsning for MLS i SAP ERP-systemet. ERP-systemer har som kjent med arbeidsflyter å gjøre.

DBSy er en metode innen MLS. Vi tror det er mulig å lage en arkitektur ut ifra DBSy-metoden, og ut i fra den lage en formell modell. Glasgow og MacEwen har i SNet-modellen, laget en formell modell basert på en ferdig laget arkitektur. Vi mener at dette kan være en mulig fremgangsmåte for å lage en ny og formell MLS-modell. På denne måten kan Forsvaret hvis ønskelig, få en modell spesielt tilpasset sine behov.

Etter BLP-modellen har det kommet svært få, nye MLS-tankeganger som kan være styrende for fremtidige systemer. Det nærmeste vi kommer er DBSy-metoden, men denne er ikke noen formell modell. Slik vi ser det, er det et stort behov for en ny, veiledende og formell MLS-modell, som kan styre utviklingen av fremtidige MLS-systemer og tilhørende mekanismer. Dette kan sette i gang utviklingen av nye systemer, og være et stort steg videre på veien mot MLS i Forsvaret.

6.5 Realiserte Multilevel Security -systemer og systemer i Forsvaret i dag

Tabell 8: Oversikt over valgte MLS-systemer.

Navn	Operativsystem	Meldingstjeneste	Fullverdig MLS	Delvis MLS	Annet
IBM – Fujifilm Medical Systems			X		
Sun Trusted Solaris v1.1	X				
Personlig Brukersystem		X			
Partisjonert fellesnivå				X	
SyBard					X
RAF's LITS			X		
AT&T's System V/MLS	X				
CMW					X

Realiserte MLS-systemer har blitt implementert med vekslende erfaringer. Få av systemene er interessante for Forsvaret i dag, hovedsaklig fordi de ikke tilfredsstiller Forsvarets krav til sikkerhet og tiltro. Logistikksystemene har i større grad enn de andre systemene mange trekk som kan brukes i et MLS-system i dag. Logistikksystemene er kanskje de mest interessante i forsvarssammenheng, på tross av at de i sin tid gikk med knakende underskudd og ble lagt på is.

En av hovedgrunnene til at prosjektene i forbindelse med Logistikksystemene gikk med underskudd, var stadige endringer av kravene. En kan vanskelig gardere seg mot kravendringer, men en kan bli flinkere til å forutse endringene. En måte å møte denne utfordringen på, kan være å lage et bedre og mer omfattende forprosjekt. I tillegg vil det utvilsomt være en fordel å studere tidligere prosjekter og erfaringer. Ved gjennomføring av store prosjekter vil det alltid være en risiko for at kravene endres underveis, særlig i tilfeller der et prosjekt strekker seg over en lang periode.

Andre eksempler på realiserte MLS-systemer er modifiserte versjoner av Unix. Det negative med disse er at de ikke tilbyr en helhetsløsning. Det vil si at de bare fungerer på enkelte områder.

CMW er et gammelt Windowsbasert system, som gjennom brukergrensesnittet gir innspill til hvordan et MLS-system kan se ut. Vi vet at CMW blant annet har blitt brukt sammen med logistikk og i ulike operative formål. Det negative med dette systemet er at det har begrensninger i bruk. CMW er ingen fullstendig MLS-løsning og er heller ikke i bruk i dag.

Sybard er et Windowsbasert system og kan derfor ikke evalueres høyere enn EAL4. Selv om tiltroen ikke er høyere enn EAL4, er det faktisk flere forsvarsrettede organisasjoner i Storbritannia som bruker denne løsningen. Dette tyder på at løsningen for øvrig er meget god. For å få en høyere evaluering enn EAL4, må QinetiQ bytte til et annet operativsystem med høyere tiltro, for eksempel Linux. Selv om tiltroen til SyBard ikke er høyere enn EAL4, kan det tenkes at noen av komponentene kan brukes i en løsning for Forsvaret.

IBMs MLS-løsning til Fujifilm Medical Systems er i stadig bruk og fungerer ifølge IBM, utmerket. Fujifilm Medical Systems har etter at de innførte MLS, oppnådd større effektivitet og et betydelig bedre samarbeid mellom sine avdelinger. Igjen er det tiltro og gjeldende sikkerhetskrav som setter en stopper for at Forsvaret kan bruke denne løsningen. Systemet hadde neppe oppnådd høy nok tiltro i en CC-evaluering til å bli et fullverdig MLS-system.

Det norske forsvaret har flere eksisterende løsninger som gir en viss MLS-funksjonalitet. Partisjonert fellesnivå gjør det for eksempel mulig å sammenkoble lavgraderte systemer med Internett. Dette var tidligere ikke tillatt; og det at regelverket åpnet for en slik sammenkobling, var absolutt et steg i riktig retning mot MLS. For at Forsvaret skal nå sin målsetning om et NbF, må en imidlertid ha sammenkobling fra Internett til HEMMELIG, hvilket dagens regelverk ikke tillater. Forsvaret har altså gjort det meste de får lov til, i forhold til gjeldende krav.

Mange av de systemene vi har gjennomgått er for gamle til å kunne satses på i dag. Vi ser likevel muligheten til å lære av styrker og svakheter ved de eldre systemene. Vi tenker da i første rekke på Logistikksystemene. Av de nyere systemene kan IBM og SyBard nevnes. Disse systemene har trolig høy nok tiltro for de fleste private foretak, og for enkelte offentlige organisasjoner. Det kan også tenkes at Forsvarets tonivåløsning kan brukes av andre enn Forsvaret.

6.6 Konsekvenser ved innføring av Multilevel Security

Vi har kommet frem til at en eventuell innføring av MLS, vil medføre til dels store forandringer både for Forsvaret som organisasjon og for den enkelte bruker av systemet.

Sikkerhetsmessig vil et MLS-system kreve god kontroll med autorisasjon av brukere. Hvis ikke dette er på plass, kan det få fatale konsekvenser. Det kan resultere i at brukere får tilgang til informasjon som de ikke skal ha innsyn i. Konsekvensene ved at sensitiv informasjon kommer på avveie, kan være svært kostbare og alvorlige for Forsvaret. I verste fall kan det bety risiko for rikets sikkerhet. For å sette dette i perspektiv vil dagens underskudd i Forsvaret bare utgjøre en brøkdel av det en slik affære kan koste.

Vårt inntrykk er at dagens løsning oppleves som tidkrevende og lite brukervennlig. MLS kan løse disse problemene, slik at brukerne slipper hyppige skiftinger mellom brukerstasjoner. Et

MLS-system kan gi de ansatte mulighet til å utføre sine oppgaver både på offentlig og sensitivt nivå, fra en og samme brukerstasjon. Videre vil et fullverdig MLS-system gjøre det mulig for de ansatte å nå den informasjonen de trenger, hvor som helst og når som helst. Dette vil bidra til bedre informasjonsflyt i organisasjonen, og til å nå målsettingen om informasjonsoverlegenhet i forhold til andre nasjoner. Slik vi ser det er MLS et ”must” for å nå denne målsettingen.

Vi antar at Forsvaret med et MLS-system, vil kunne minske mengden med dupleks informasjon, og slippe ned en del BEGRENSET informasjon fra HEMMELIGE nett. En vil da unngå dupleks lagringer av lik informasjon. Det kom frem i spørreundersøkelsen at det i dag er mye dupleks informasjon mellom det nasjonale HEMMELIGE nettet og NATO SECRET-nettet, faktisk mer enn sytti prosent. Dette kan unngås ved å gi NATO-graderinger i større grad.

Det stilles høye krav til tiltro på informasjonen i et MLS-system. Dette medfører at brukerne tillegges et stort ansvar, i og med at det er de som lagrer og sender ut informasjonen. Opplæring av brukerne bør derfor tillegges stor vekt ved en MLS-innføring. En slik opplæring vil sannsynligvis være ressurskrevende, både med hensyn til kostnader og personellbehov. Et annet moment med opplæringen, er at den kan være med på å kvalitetssikre personellet som skal jobbe på systemet.

Utvikling og implementering av et MLS-system vil kreve enorme ressurser. Hovedårsakene til dette er at det ikke finnes noen kommersiell løsning, og fordi Forsvaret trenger svært høy tiltro til et slikt system. Videre finnes det ikke høyt nok sertifiserte komponenter til å bygge et slik system. Forsvaret må derfor få utviklet egne komponenter. Kompetanse for å utføre dette må hentes inn utenfra, og vil medføre store kostnader. Det store spørsmålet er hvem som skal betale regningen. Forsvaret vil aldri få mulighet til å koste den alene, og en utvikler eller leverandør vil neppe påta seg hele kostnaden. Til det er markedet for lite. Det kan være en mulighet å dele kostnadene mellom flere interessenter, så som utvikler, leverandør, Forsvaret og kanskje NSM. En annen mulighet er at NATO-landene slår seg sammen og utvikler et felles system, og deler kostnadene seg imellom. Videre kan det være mulig å kommersialisere det hele ved å få med representanter fra Forsvaret inn i for eksempel SAP. SAP jobber som kjent med MLS-problematikken, under DEIG.

En eventuell innføring av MLS, vil medføre store, fortrinnsvis positive, konsekvenser for Forsvaret. Sannsynligvis vil MLS bidra til større effektivitet, bedre oversikt og bedre informasjonsflyt. Selv om det er en kostbar investering, både med hensyn til utvikling, implementering og opplæring, tror vi at det på sikt vil bli en lønnsom investering for Forsvaret.

6.7 Validitet

Ordet validitet betyr gyldighet eller relevans, og berører både teoriplanet og empiriplanet. Kort sagt kan vi si at problemstillingene tilhører teoriplanet, mens tolkningen foregår på empiriplanet. Empiri er vitenskapelige undersøkelser av virkeligheten.

For å vurdere oppgavens validitet, har vi gått tilbake og vurdert undersøkelsesopplegget. I og med at vi har behandlet delproblemene med ulike tilnærminger, har vi valgt å se på styrker og svakheter ved de enkelte delproblemene hver for seg. Siden den første kvalitative undersøkelsen ble benyttet i alle tre delproblemene, har vi omtalt denne først.

6.7.1 Kvalitativ undersøkelse 1

Dette var en kvalitativ undersøkelse, basert på få og fyldige intervjuer. Vi er derfor sikre på at alle forstod spørsmålene. For å kvalitetssikre svarene har intervjuobjektene lest igjennom resultatene i etterkant.

Det kan være at vi burde ha delt undersøkelsen inn i tre mindre undersøkelser. På denne måten kunne vi ha funnet intervjuobjekter med spesielle kunnskaper innen hvert enkelt delproblem. Vi vurderte dette, men forkastet tanken av ulike årsaker.

Vi ønsket fortrinnsvis å gjennomføre kvalitative intervjuer, spesielt med tanke på at vi hadde lite kunnskaper om MLS i starten, og trengte å tilegne oss all den kunnskap vi hadde mulighet til. Kvalitative intervjuer ville gi oss en bredere forståelse av MLS generelt, og et innblikk i hvilke tanker som verserer om dette i Forsvaret. Det å gjennomføre tre undersøkelser i stedet for en, ville ha tatt mer tid, og sannsynligvis ført til dårligere kvalitet på hvert enkelt intervju. Undersøkelsene hadde blitt mindre omfattende, og vi hadde hatt mindre tid til hvert intervjuobjekt.

Videre stiller vi oss tvilende til om resultatene hadde blitt bedre, dersom vi hadde gjennomført tre i stedet for en undersøkelse. I forbindelse med det første delproblemet burde vi ha intervjuet folk i NSM, hvilket viste seg umulig å få til. For å få fyldige svar til det andre delproblemet måtte vi ha fått tak i eksperter på MLS. De fleste av dem befinner seg i utlandet og kan være vanskelige å få tak i. Med andre ord ville vi trolig ha brukt betydelig med tid på å finne rette intervjuobjekter. I tillegg ville det medført mer reising og tre ganger så mange intervjuer og telefoner. Vi vurderte det dit hen at dette ville gå utover kvaliteten på intervjuene, og valgte derfor å utføre en felles undersøkelse som omfattet alle tre delproblemene.

Når det gjelder utvalget, så bestod det av fem personer fra Program Golf og FLO/IKT. Disse har alle spesiell kunnskap innen sikkerhet og IKT, og hadde gode forutsetninger for å svare på de fleste spørsmålene i undersøkelsen.

Vi gjennomførte intervjuene på bakgrunn av en intervjuguide. Her hadde vi skrevet opp spørsmål som vi ønsket å stille. Videre hadde vi satt opp svaralternativer under hvert spørsmål. På denne måten fikk vi stilt alle spørsmål som skulle stilles, og vi fikk i gang samtale rundt de ulike emnene. Intervjuene ble tapet og skrevet ned; deretter leste intervjuobjektene igjennom og kvalitetssikret resultatene.

6.7.2 Delproblem 1

Undersøkelsen ble hovedsakelig gjort med bakgrunn i dybdeintervjuer blant ansatte innen sikkerhet og IKT i Forsvaret.

Slik vi ser det, hadde det vært et stort pluss om vi hadde fått kontakt med, og informasjon fra, NSM. Da NSM har ansvaret for å tolke Sikkerhetsloven og å utarbeide tilhørende forskrifter og veiledninger, er det høyst sannsynlig de som kjenner lovverket best. Videre jobber de tett opp mot NATOs lovverk, og kunne ha gitt oss fyldig informasjon om dette. Det mest interessante hadde vært å få et innblikk i hvilke tanker NSM har om MLS i fremtiden. Et møte eller en mulighet til å utføre intervjuer med ansatte i NSM, hadde trolig gitt oss en bredere forståelse av gjeldende lover og regler. Dette kunne ha bidratt til en fyldigere og mer nøyaktig redegjørelse av gjeldende krav. Vi lyktes dessverre ikke i å få kontakt med NSM. Vi mener likevel at resultatene gir et riktig bilde av hvilke krav som Forsvaret må forholde seg til.

Både sikkerhetsbestemmelser og evalueringskriterier er noe som endrer seg over tid. Resultatene er gyldige i dag, men kan forandres i morgen. Det kommer stadig endringer til Sikkerhetsloven og dens forskrifter og veiledninger. I oppgaven viser vi til bestemte paragrafer i bestemmelsene. Både Sikkerhetsloven og dens forskrifter og veiledninger er tilgjengelig på Internett, og det er derfor enkelt å finne ut om det har blitt gjort forandringer.

Når det gjelder evalueringskriteriene, så endres disse også med tiden. Endringene er muligens ikke store, men en må være oppmerksom på at det kan skje endringer. De siste endringene i CC ble gjennomført i 1999. Et annet moment er at evalueringskriteriene iblant skiftes ut. CC ble innført i 1991, og det kan tenkes at de med tid og stunder blir skiftet ut.

Vår oppgave er skrevet for Forsvaret, og er naturligvis hovedsakelig gjeldende for det. NATOs bestemmelser gjelder kun for systemer som er koblet opp mot NATOs systemer. Når det gjelder Sikkerhetsloven og gjeldende krav til sammenkobling av systemer med gradert informasjonsflyt, så er de styrende for alle offentlige virksomheter. Det er bare private foretak som ikke trenger å følge Sikkerhetsloven med forskrifter og veiledninger.

6.7.3 Delproblem 2

Når det gjelder intervjuene i forbindelse med det andre delproblemet, så ga de mindre utbytte enn forventet. Ingen av intervjuobjektene kjente til teorier og strategier innen MLS. Vi visste

på forhånd at det ikke var MLS-eksperter vi skulle intervjue, og var forberedte på at kunnskapene innen de ulike fagområdene kunne variere fra person til person.

Det kan tenkes at det hadde vært en fordel å intervjue folk med mer dyptgående kunnskaper om MLS. Dette vurderte vi, men opplevde problemer med å få tak i såkalte eksperter på området. Dessuten har de som jobber med MLS ofte spesiell kunnskap om en spesifikk modell eller et spesielt system, men ikke nødvendigvis kjennskap til andre områder innen MLS. Et annet moment er at de som har kunnskap om MLS, ofte ikke kjenner til hvilke utfordringer MLS byr på i forsvarsmiljøer. Det har i løpet av årene blitt laget mange modeller og realiserte systemer, men de fleste uten tanke på bruk i forsvarssammenheng. Forøvrig befinner de aller fleste ekspertene seg i utlandet, hvilket byr på problemer i forbindelse med tidsforskjeller og språk. Vi valgte derfor å foreta undersøkelsen blant folk i Forsvaret, og heller stille spørsmål til enkelte eksperter via e-post.

Intervjuene ga som sagt lite resultater i forhold til teorier og strategier innen MLS. Resultatene ble derfor i større grad enn planlagt, basert på litteratursøk med påfølgende utvelgelser og vurderinger. Det kan være at resultatene hadde blitt annerledes med flere innspill fra intervjuene. Vi har ingen garanti for at vi har valgt ut de viktigste teoriene og strategiene. Utvalget er tatt ut ifra egne vurderinger, med bakgrunn i tilegnet kunnskap gjennom prosjektet.

Om vi hadde valgt andre, kanskje mindre kjente, og nyere modeller, kunne resultatene teoretisk sett ha blitt annerledes. Vi tror likevel ikke at et annet utvalg ville hatt nevneverdig innvirkning på utfallet av oppgaven. I beste fall kunne vi ha funnet en modell som tilfredstilte Forsvarets behov, men etter våre erfaringer anser vi den muligheten som mikroskopisk.

Vi mener at utvalget av teorier og strategier gir et godt bilde av hvordan MLS-tankegangen har utviklet seg gjennom årene. Når det gjelder realiserte MLS-systemer, så bygger disse resultatene i hovedsak på intervjuene.

Slik vi ser det, er flere av modellene relevante for virksomheter utover Forsvaret. Dette gjelder blant andre DBSy-modellen og arbeidsflytmodellene. De formelle modellene vi har presentert bruker MAC, som er en streng politikk. Vi har valgt MAC på grunn av at Forsvaret stiller svært høye krav til sikkerhet. Andre virksomheter har ofte lavere krav til sikkerhet, og vil derfor kanskje velge DAC eller RBAC, som er mindre strenge politikker.

6.7.4 Delproblem 3

Resultatene og arbeidet med det tredje delproblemet, er basert på to kvalitative undersøkelser. Den første ble utført blant ikke-operativt personell som jobber med sikkerhet og IKT, og den andre ble utført blant operativt personell som jobber på graderte systemer til daglig.

Det er mulig at et større og bredere utvalg av intervjuobjekter kunne ha gitt andre resultater. Av de som jobber på graderte nett til daglig, har vi kun intervjuet fire personer. Dette er et forholdsvis lite utvalg, særlig med tanke på at de fleste jobber innenfor samme avdeling. Ser vi det i sammenheng med resultatene fra intervjuene med de fem personene som jobber med sikkerhet og IKT, mener vi likevel at vi har et representativt utvalg. Vi har fått synspunkter fra til sammen ni personer. Blant disse finnes både operativt og ikke-operativt personell, med svært varierte bakgrunner og kunnskaper.

Resultatene henspeiler på situasjonen i Forsvaret i dag. Det kommer stadig nye systemer i Forsvaret, særlig på grunn av arbeidet med å få til et FIF. Likevel antar vi at det ikke blir store forandringer med tanke på hvordan det er å jobbe på de graderte systemene, før Forsvaret eventuelt implementerer MLS eller MSL.

Resultatene er meget relevante for andre forsvarsmiljøer, men vil også gi god nytte for sivile foretak. Kravene til sikkerhet og tiltro er i de fleste tilfeller langt høyere i forsvarsmiljøer enn i det sivile. Når det gjelder konsekvensene utover dette, tror vi at de vil samsvare med konsekvenser i sivile miljøer. Konsekvensene som dreier seg om brukervennlighet, effektivitet og informasjonsflyt, vil høyst sannsynlig gjelde i de aller fleste tilfeller der en innfører MLS.

Kvalitativ undersøkelse 2

Vi vurderte i første omgang å gjennomføre en kvantitativ undersøkelse med mange informanter. Dette viste seg imidlertid vanskelig, siden det er et begrenset antall personer som jobber på graderte nett til daglig. Samtidig var mange restriktive til å være med på en slik undersøkelse på grunn av stort arbeidspress og dårlig tid. I tillegg stilte mange seg negative på grunn av undersøkelsens art, med direkte spørsmål om graderte nett og bruken av dem.

Vi bestemte oss derfor for å gjennomføre en kvalitativ undersøkelse. På bakgrunn av bekjentskaper kom vi i kontakt med fire personer som stilte seg positive til å la seg intervjue, med forutsetning om at de kunne være anonyme. Utvalget bestod av folk fra Forsvarets spesialstyrker i innland og utland, og intervjuene måtte derfor foretas skriftlig via e-post. Dette medvirket til at personene oppfattet spørsmålene noe forskjellig. Videre var det store variasjoner i hvor fyldige besvarelsene ble.

Det hadde helt klart gitt bedre resultater dersom intervjuene hadde vært foretatt ved personlig fremmøte eller per telefon. Vi kunnet da ha forsikret oss om at alle forstod spørsmålene likt. Videre hadde en personlig samtale gitt mer utfyllende svar. Ved en skriftlig undersøkelse er det alltid noen som velger den enkle utveien og hopper over utfylling i merknadsfeltene. Det var dessverre ikke mulig å få til personlige intervjuer med den gjeldende gruppen.

Et annet moment er at et bredere utvalg kunne ha gitt andre resultater. Vi kunne med fordel ha supplert med folk fra andre avdelinger og med andre arbeidsoppgaver. Da hadde vi fått et bredere og kanskje riktigere bilde av hvordan brukerne av graderte nett oppfatter dagens løsning. Våre resultater representerer synspunkter kun fra et fåtall av de ansatte, og de fleste fra en og samme avdeling. Det positive med vårt utvalg, er at alle har mye erfaring. De fleste har vært i utenlandstjeneste og har vært i operativ tjeneste i lengre tid, og er trolig blant de som jobber mest på graderte nett i det norske forsvaret. Etter vårt syn er dette en svært viktig gruppe å ta hensyn til, ved en eventuell innføring av MLS i Forsvaret.

Svarene fra intervjuobjektene er basert på erfaring fra bruk av nåværende systemer i Forsvaret. Det betyr at synspunktene vedrørende hvordan nåværende systemer fungerer og oppleves, er godt begrunnet. Videre hadde de mange tanker om hva som er dårlig, og hva som med fordel kan bli bedre. Personene hadde imidlertid ikke forutsetninger for å mene noe om fremtidsutsikter for MLS. Grunnen til at vi stilte spørsmål om dette, var for å få greie på hvilke oppfatninger som verserer ute i bruket.

7 Konklusjon

Forsvaret har en målsetting om å bli et NbF, hvilket krever MLS. Vi har kartlagt dagens MLS-situasjon i forhold til hvilke krav Forsvaret må forholde seg til, hvilke teorier og strategier som finnes, samt hvilke konsekvenser en MLS-innføring kan få for Forsvaret.

Gjeldende sikkerhetskrav tillater ikke sammenkobling av systemer med forskjellige graderingsnivåer. Dette betyr at Forsvaret, med gjeldende krav, ikke kan få godkjent en fullverdig MLS-løsning. For at dette skal bli mulig, må sikkerhetskravene endres.

Evaluering av systemer er en omfattende og svært kostnadskrevende prosess. CC er gjeldende evalueringskriterier. Disse begynner å bli gamle, og vi mener at Forsvaret bør vurdere om de er modne for utskifting. I så fall bør Forsvaret gå inn for å påvirke en fornying av CC, eller en utvikling av nye kriterier.

Vi har presentert teorier og strategier som gir en historisk oversikt over MLS. Svært få av de eldre modellene kan brukes i et moderne MLS-system. De viser likevel hva som har blitt gjort tidligere, hva som har fungert og hva som ikke har fungert. Dette kan være viktige bidrag i utvikling av nye modeller og systemer. På bakgrunn av de modellene vi har studert, ser det ut til å være behov for en ny formell modell, som kan legges til grunn for fremtidige MLS-systemer.

Videre har vi presentert realiserte systemer. Disse gir i likhet med modellene, et bilde av hva som er gjort tidligere, både positive og negative erfaringer. Blant de nye og bedre løsningene, er blant andre SyBard og IBMs MLS-løsning til Fujifilm Medical Systems. Disse systemene har høy nok tiltro for de fleste private foretak, og for enkelte offentlige organisasjoner. De tilfredsstiller dessverre ikke Forsvarets krav til tiltro.

Utvikling og innføring av et MLS-system er et svært kostbart foretak. For å redusere noe av kostnaden, kan Forsvaret inngå en kostnadsdeling med utvikler, leverandør og eventuelt NSM. Videre er det en mulighet å gå sammen om en kostnadsdeling med andre NATO-land.

7.1 Forslag til videre fremdrift

Etter vår mening bør Forsvaret lage en plan for arbeidet mot en fullverdig MLS-løsning, som er en forutsetning for et NbF. Forsvaret har vist initiativ ved å starte denne masteroppgaven. Veien mot MLS er imidlertid lang. Ut i fra erfaringer og tilegnet kunnskap gjennom arbeidet med oppgaven, har vi satt opp et forslag til hvordan Forsvaret kan gå frem i det videre arbeidet mot MLS.

I første omgang må noen tildeles spesifikt ansvar for det videre arbeidet med MLS. Deretter bør Forsvarets behov i forhold til informasjonsflyt, kartlegges. På bakgrunn av dette bør det fastsettes mål og utarbeides en plan for arbeidet fremover.

Per i dag er det delte meninger vedrørende både sikkerhetskrav og evalueringskrav. Slik vi ser det, må Forsvaret ta stilling til hva de mener om gjeldende krav. Bør sikkerhetskravene endres? Og bør evalueringskriteriene endres? En slik endring er faktisk en forutsetning for å få til en fullverdig MLS-løsning for Forsvaret.

Videre bør en se på muligheten for å alliere seg med andre i NATO som ønsker å oppnå det samme, med hensyn til endringer i gjeldende krav. Norge er en liten nasjon med begrenset påvirkningskraft; ved å stå sammen med andre vil mulighetene for gjennomslag øke betraktelig.

Etter å ha klarlagt hvordan de andre nasjonene forholder seg til gjeldende krav, kan en starte arbeidet med en eventuell endring av gjeldende bestemmelser, både sikkerhetskrav og evalueringskriterier. Vi tror at det beste vil være å starte med påvirkning opp mot NATO. Det er da viktig på forhånd å ha en klar formening om nøyaktig hva en ønsker å endre.

Det er mange nasjoner i NATO som ivrer etter å få til en fullverdig MLS-løsning. Norge bør starte et samarbeid med andre NATO-land om utvikling av et felles MLS-system og tilhørende komponenter. Et slikt samarbeid vil gi flere ressurser til arbeidet, og trolig raskere progresjon, enn om Norge står alene.

Når det gjelder valg av metode, strategi og modell, er dette en omfattende prosess. Dette bør velges i samarbeid med utviklere og leverandører. Sannsynligvis må det utarbeides en ny modell, da de fleste eksisterende modeller enten er gamle og utdaterte, eller ikke tilfredsstiller kravene til et fullverdig MLS-system. Det kan også være en mulighet å jobbe videre ut ifra DBSy-metoden.

Etter å ha utarbeidet et formalisert system, står evalueringen for tur. Per i dag er det CC som er gjeldende, men det kan være at det innen evalueringen står for tur, har blitt utarbeidet nye evalueringskriterier.

Til slutt står implementering av systemet for tur. I denne forbindelse bør det gjennomføres en grundig opplæring av alle som skal benytte systemet, det vil si hele Forsvaret.

Vi mener at det er svært viktig at Forsvaret så raskt som mulig setter seg inn i problematikken rundt MLS, etablerer kontakter i MLS-miljøet, og får satt MLS på dagsordenen. Dess før en starter arbeidet med MLS, jo raskere vil antageligvis en løsning komme. Arbeidet med å få realisert MLS i Forsvaret, er en svært kostbar og tidkrevende prosess. Vi mener likevel at

fordelene er langt større enn ulempene. Dessuten tror vi at MLS på sikt vil være en lønnsom investering for Forsvaret.

8 Forkortelser

AT&T	American Telephone and Telegraph Company
BLP	Bell-LaPadula
C2G	The Command and Control Guard
CC	Common Criteria, Se CCITSE
CCITSE	Common Criteria for Information Technology Security Evaluation
CCR	Container Clearence Required
CMW	Compared mode workstations
CTCPEC	Canadian Criteria
DAC	Discretionary Access Control
DERA	Defence Evaluation And Research Agency
EAL	Evaluation Assurance Level
ERP	Enterprise Resource Planning
DBSy	Domain Based Security
DEIG	Defence Interest Group
FC	US Federal Criteria
FIF	Felles Integrert Forvaltningssystem
FLO/IKT	Forsvarets Logistikkorganisasjon/Informasjons- og kommunikasjons- teknologi
FP1	Forprosjekt 1
FP2	Forprosjekt 2
IACS	Infosec Assurance and Certification Services
IBM	International Business Machines
ITSEC	Information Technology Security Evaluation Criteria
KUN	Kommunikasjonsundernettverk
MAC	Mandatory Access Control
MMS	Military Message Modell
MLS	Multilevel Security
MoD	Ministry of Defence
MSL	Multiple-Single-Levels el. Multi System Level
NATO	North Atlantic Treaty Organisation
NbF	Nettverksbasert Forsvar
NPD	Named Protection Domain
NRL	Navy Research Laboratory
NSM	Nasjonal Sikkerhetsmyndighet
PBS	Personlig Brukersystem
RAF's LITS	The Royal Air Force's Logistics Information Technology System
RBAC	Role-Based Access Control
SAP	Systems, Applications, Products
SCOMP	The Secure Communications Processor
SQL	Structured Query Language
TOE	Target of Evaluation
TPFDD	the Time-Phased Force Deployment Data
TCSEC	The Trusted Computer Security Evaluation Criteria (Orange Book)
WFMS	Workflow Management System

9 Litteraturliste

CC (Common Criteria). (2003). Sist tilgjengelig 21. april, 2005, fra http://csrc.nist.gov/cc/

IACS (Infosec Assurance and Certification Services). (2005) Sist tilgjengelig 21. april, 2005, fra http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=11

ITSEC (Information Technology Security Evaluation Criteria). (1991). Sist tilgjengelig 21. april, 2005, fra http://www.iwar.org.uk/comsec/resources/standards/itsec.htm

Fujifilm Medical Systems USA becomes the picture of collaboration. (n.d.). Sist tilgjengelig 13. mai 2005 fra http://www-306.ibm.com/software/success/cssdb.nsf/CS/CDIR-5T2LZ3?OpenDocument&Site=default

METEOR prosjekt hjemmeside. (n.d.). Sist tilgjengelig 19. april, 2005, fra http://lsdis.cs.uga.edu/proj/meteor/meteor.html

Program Golf. (n.d.). Sist tilgjengelig 27. oktober, 2004, fra http://www.mil.no/fst/golf/start/.

TCSEC (The Trusted Computer Security Evaluation Criteria). (1985). Sist tilgjengelig 21. april, 2005, fra http://www.boran.com/security/tcsec.html

Trusted Network Interpretiation. (1987). Sist tilgjengelig: 25. april 2005, Fra: *http://www.fas.org/irp/nsa/rainbow/tg005.htm*

Ames, S.R., Biba, K.J., Bradshaw, F.T., Gilligan, J.M., Ogden, W.F., Rounds, W.C., Schaeffer, D.D., Schaen, S.I., Shumway, D.G. & Walter, K.G. (1975). Structuered specification of a Security Kernel. *International conference on Reliable software,* 285 – 293

Ames, S.R. & Oestreicher, D.R. (1978). Design of a Message Processing System for a Multilevel Secure Environment. *AFIPS Nat. Computer Conf, AFIPS Press,* 47, 765-771

Amoroso, E. (1994). *Fundamentals of Computer Security Technology,* Prentice Hall.

Anderson, R. J. (2001). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley Computer Publishing

Atluri, V., Bertino, E. & Huang, W-K. (1997). An Execution Model for Multilevel Secure Workflows. *IFIP Working Conference on Database Security.*

Atluri, V., Bertino, E. & Huang, W-K. (2000). A Semantic Based Execution Model for Multilevel Secure Workflows. *Journal of Computer Security, IOS Press,* 8, 3-41

Baldwin, R.W. (1990). Naming and grouping privileges to simplify security management In large database. *IEEE Computer Society Symposium on Research in Security and Privacy*, 61–70

Bell, D.E., & LaPadula, L.J. (1973) Secure Computer Systems: Mathematical Foundations. *ESD-TR-73-278, Hanscom Field, Bedford,* 1

Bell, D.E. & LaPadula, L.J. (1976). Secure Computer Systems: Unified Exposition and Multics Interpretation. *Mitre Technical Report-2997, Mitre Corporation,* Bedford, MA.

Biba, K.J. (1977). Integrity Considerations for Secure Computer Systems. *Mitre Technical Report-3153,* Mitre Corporation

Bonneau, C.I-I. (1980). Secure Communications Processor Kernel Sofh.vare. *Detailed Spec@cation, Honeywell Inc., Avionics Division,* Part I, Rev.D

Brewer, D.F.C. & Nash, M.J. (1989). The Chinese Wall Security Policy. *IEEE Computer Society Symposium on Security and Privacy*, 206-214

Castano, S., Fugini, M.G., Martella, G. & Samarati, P. (1995). Database Security. *Addison Wesley, ACM Press*

Clark, D.D., Saltzer, J.H. & Schroeder, M.D. (1977). The Multics kernel design project. *Sixth ACM Symposium on Operating systems principles,* 43 – 56

Clark, D.D. & Wilson, D.R. (1987). A Comparsion of Commercial and Military Computer security Policies. *IEEE Symposium on Security And Privacy*, 184-194

Cohen, F. (1987). Computer Viruses - Theory and Experiments. *IFIP-TC11 "Computers and Security",* 6, 22-35

Cooper, L.F. (2004). Multi-Level Security Strategies for the Federal Government. *Larstan Business Reports*.

Dalland, O. (2000). *Metode og oppgaveskriving for studenter*. Universitetsforlaget, Oslo.

Denning, D.E. (1976). A lattice model of secure information flow. *Communications of the ACM archive,* 19(5), 236 – 243

Doan, T., Demurjian, S., Ting, T.C. & Ketterl, A. (2004). Mac and UML for Secure Software Design. *ACM workshop on Formal methods in security engineering*

Farber, D.A & Popek, G.J. (1978). A model for verification of data security in operating systems. *Communications of the ACM archive,* 21(9), 737 – 749

Feiertag, R.J., Levitt, K.N. & Robinson, L. (1977).Proving Multilevel Security of a System Design. *6th ACM Symposium on Operating Syst. Principles, ACM SIGOPS Operating Syst.,* 11(5), 57-65

Foreskrift om informasjonssikkerhet. (2001). Cappelen akademiske forlag.

Glasgow, J. I., Ouabdesselam, F., MacEwen, G. H., & Mercouris, T. (1984). Specifying multilevel security in a distributed system. *National Computer Security Conference in Gaithersburg,* 319-340

Glasgow, J.I. & MacEwen, G.H. (1987). The Development and proof of a Formal specification for a Multilevel Secure System. *Queen's University, Kingston Canada.*

Harrison, W., Ruzzo, W. & Ullman, J. (1976). Protection in operating systems. *Communications of the ACM, 19(8),* 461-471

Heydon, A., Maimone, M.W., Tygar, J.D., Wing, J.M. & Zaremski, A.M. (1990). Mirò: Visual Specification of Security. *IEEE Transactions on Software Engineering*, 16(10), 1185-1197

Hughes, K.J. (2002). Domain Based Security: Enabling security at the level of applications and business processes. *Sist tilgjengelig: 19. april 2005, Fra: Http://www.qinetiq.com/home_enterprise_security/infosec_strategy/white_papers.htm*

Johannessen, A., Kristoffersen, L., Tufte, P.A. (2004), *Forskningsmetode for økonomisk*

-administrative fag, Abstrakt forlag AS.

Kang, M. H., Froscher, J. & Eppinger, B. (1998). Toward an Infrastructure for MLS Distributed Computing. *14th Annual Computer Security Applications Conference, IEEE Computer Society*

Kang, M. H., Froscher, J. N. & Moskowitz, I. S. (1997). An Architecture for Multilevel Secure Interoperability. *13th Annual Computer Security Applications Conference, IEEE Computer Society*

Kang, M. H., Moskowitz, IS & Lee, D. C. (1996). A Network Pump. *IEEE Transactions on Software Engineering*, 329-338

Kang, M. H., Froscher, J., Eppinger, B. J. & Moskowitz, I. S. (1999). A strategy for an MLS Workflow Management System. *13th IFIP Conference on Database Security*

Kemmerer, R.A., Popek, G.J. & Walker, B.J. (1979). Specification and verification of the UCLA Unix security kernel. 7th *ACM symposium on Operating systems principles,* 64 - 65

Kochut, K., Sheth, A., & Miller, J. (1998). ORBWork: A CORBA-Based Fully Distributed, Scalable and Dynamic Workflow Enactment Service for METEOR. *UGA-CS-TR-98-006, Technical Report,Department of Computer Science, University of Georgia*

Landwehr, C.E. (1981). A survey of formal Models for computer security. *ACM Computing Surveys,* 13(3), 247-278

Landwehr, C.E., Heitmeyer, C.L. & Mclean, J. (1984). A Security Model for Military Message systems. *ACM Trans. On computer systems,* 9(3), 198-222.

Lampson, B.W. (1971). Protection. *5th Princeton Syrup. Information Sciences and Systems*, 437-443

Lampson, B.W. (1973). A note on the confinement Problem. *Communications of the ACM,* 16(10), 613-615

Lipton, R.J. & Snyder, L. (1977). A Linear Time Algorithm for Deciding Subject Security. *Journal of the ACM (JACM),* 24(3), 455-464

Mackenzie, D. & Pottinger, G. (1997). Mathematics, Technology, and Trust: Formal Verification, Computer Security,and the U.S. Military. *IEEE Annals of the History of Computing,* 19(3)

Millen, J.K. (1976). Security Kernel Validation in Practice. *Communications of the ACM archive,* 19 (5), 243-250

NSM (Nasjonal Sikkerhetsmyndighet).(2004). *Veiledning i grunnleggende sikkerhetsarkitektur og -funksjonalitet for PARTISJONERT operasjonsmåte.*

Olsson, H. og Sørensen, S. (2003), *Forskningsprosessen Kvalitative og kvantitative perspektiver*, Gyldendal Norsk Forlag AS.

Pedersen, R.A, Bø, S.E., Haraldseid, E., Sletten, B., Egeland, H.P., Christoffersen, Ø., Meland, G. (2004). FIF som del av et Nettverksbasert Forsvar. *Internt Forsvarsdokument*

Pomeroy, B. & Wiseman, S. (1998). Private Desktops and Shared Store. *Presented at the 14th*

Annual Computer Security Applications Confrence, Scottsdale Arizona

Ren, J. (2004). Modular Security: Design and Analysis. *Institute for Software Research, University of California, Irvine, ISR Technical Report # UCI-ISR-04-4*

Robinson, C.L. (2001). Security Requirements Models to Support the Accreditation Process. *Presented at 2nd Annual Sunningdale Accreditor's Conference, 10th – 11th September*

Sandhu, R.S. (1992). The Typed Access Matrix Model. *IEEE Symposium on Security and Privacy*

Samarati, P. & S.d., Vimercati, C.d. (2001). Access Control: Policies, Models, and Mechanisms, in Foundations of Security Analysis and Design: Tutorial Lectures. *Springer-Verlag Heidelberg*, 137-196

Saltzer, J.H. (1974). Protection and the control of information sharing in multics. *Communications of the ACM archive,* 17(7), 388 - 402

Schroeder, M.D. (1975). Engineering a security kernel for Multics. *5th ACM Symposium on Operating systems principles,* 25 - 32

Schroeder, M.D., Clark, D.D. & Saltzer, J.H. (1977)The Multics Kernel Design Project. *6t ACM Symposium on Operating Systems Principles, ACM SIGOPS Operating Systems,* 11 (5), 43-56.

Sikkerhetsloven (Lov om forebyggende sikkerhetstjeneste samt Forskrifter).(2001). Cappelen akademiske forlag.

Smith, R. (23.02.2005). *Introduction to Multilevel Security av Dr. Rick Smith*. Sist tilgjengelig 20. april 2005, fra http://www.cs.stthomas.edu/faculty/resmith/r/mls/m1intro.html

Snyder, L. (1977). On the synthesis and analysis of protection systems. *6th ACM Symposium on Operating systems principles,* 141-150

Stegmann, C. (1997). A Framework for Authorization Policie. Professional Thesis, *Institut Eurécom.*

Varadharajan, V. (1990). A Multilevel Security Model for Networks. *Hewelett-Packard Labratories, Bristol, U.K.*

Walter, K.G., Ogden, W.F., Rounds, W.C., Bradshaw, F.T., Ames, S.R. & Shumway, D.G. (1974). PrimitiveModels for Computer Security. *ESD-TR-74-1 17, AF/ESD L.G. Hanscom Field, Bedford*

Warrener, K. (2003). Facilitating Risk Balance - An Architectural Approach. *Presentert på 15th annual Canadian Information Technology Security Symposium 15th May 2003*

Weissman, C. (1969). Security controls in the ADEPT-50 time sharing system. *AFIPS Fall Jt Computer Conf., AFIPS Press,* 35, 119-133.

Woo, T. Y. C. & Lam, S. S. (1993). Authorizations in distributed systems: A new approach. *Journal of Computer Security*, 2(3), 107–136.

10 Vedlegg

Vedlegg A: Intervjuguide til kvalitativ undersøkelse 1

Vedlegg B: Resultater fra kvalitativ undersøkelse 1

Vedlegg C: Spørreskjema til kvalitativ undersøkelse 2

Vedlegg D: Skjematiske resultater til kvalitativ undersøkelse 2

Vedlegg A: Intervjuguide til kvalitativ undersøkelse 1

Intervjuguide

Multilevel Security (MLS): Systemer med gradert informasjonsflyt

Intervjuserie nummer 1, våren 2005.

Varighet per intervju: ca. 1 time.

Innledende spørsmål:

1. Navn?
2. Stilling/tittel?
3. Utdannelse og bakgrunn?

Del 1: Forsvarets krav til systemer som sammenkobler informasjon med ulik sikkerhetsgradering.

Slik vi har forstått situasjonen, har MLS vært et tema i internasjonal forsvarssammenheng i mange år. Det jobbes stadig med å lage en MLS-løsning som er god nok, men dette har foreløpig ikke latt seg gjennomføre. Det finnes mange og omfattende sikkerhetskrav som Forsvaret må forholde seg til, blant annet Sikkerhetsloven med forskrifter og veiledninger, samt føringer fra NATO.

1. **Er det de gjeldende sikkerhetskravene som hindrer Forsvaret i å ta i bruk MLS?**
    a. Ja.
    b. Nei:
        i. Teknologien er ikke god nok til å ta i bruk MLS.
        ii. Forsvaret trenger strengt tatt ikke MLS.
        iii. Annet.
    c. Vet ikke.

Forsvaret må som nevnt tidligere, forholde seg til gjeldende sikkerhetsbestemmelser vedrørende en eventuell innføring av MLS.

2. Eventuelt hvilke sikkerhetskrav er de mest avgjørende?

a. Sikkerhetsloven med forskrifter og veiledinger.
b. NATO-krav.
c. Andre.

Er enkelte deler av loven/forskriftene/veiledningene mer avgjørende enn andre?
Hvilke deler av NATOSs krav er mest avgjørende?

Dagens MLS-løsninger tilfredsstiller ikke gjeldende sikkerhetsbestemmelser som Forsvaret må forholde seg til. Det kan være en mulighet å endre enkelte bestemmelser eller å senke kravene, og dermed åpne for en mulig innføring av MLS.

3. Hvilken betydning vil det ha dersom nåværende sikkerhetskrav senkes?

a. Forsvaret vil bli mindre sikkert.
b. Det vil åpne mulighetene for å innføre MLS.
c. Ingen betydning.
d. Vet ikke

Hvilke deler av kravene vil det i så fall være aktuelt å endre?

4. Jobbes det med å endre disse kravene?

a. Ja:
    i. NSM jobber med dette.
    ii. FSA jobber med dette.
    iii. NATO jobber med dette.
    iv. Andre.
b. Nei.

Er det noen som forsøker å påvirke i noen retning?
Er det helt uaktuelt å endre disse kravene?
Hva med policy?

MLS er foreløpig, så vidt vi vet, ikke innført i forsvarssammenheng noe sted. Videre er det tydelig at MLS er noe som forsvarsnasjoner i NATO bruker store ressurser på og ønsker å innføre. Det kan selvsagt være ulike årsaker til at innføringen av MLS lar vente på seg, og da må man se på hva som kan gjøres for å bli kvitt hindringene.

5. **Er det nødvendig å endre sikkerhetskravene for å implementere MLS i Forsvaret?**
    a. Ja:
        i. Det er helt nødvendig.
        ii. Det kan forenkle og forkorte prosessen.
    b. Nei.

    Eventuelt hvilke krav må endres.

Del 2: Kartlegging av MLS-teorier og strategier.

MLS har vært forsket på i flere tiår, og det har etter hvert blitt publisert mange modeller, arkitekturer og strategier på området. Noen av de er gamle og andre er forholdsvis nye. Vi har listet opp noen av de vi har funnet gjennom vårt kartleggingsarbeid.

1. **Det finnes mange teoretiske modeller/arkitekturer/strategier innen MLS. Er det noen av disse som betegnes som bedre enn andre? Begrunnelse.**
    a. Ja:
        i. Bell-LaPadula
        ii. The domain model – DERA,UK
        iii. UCLA data secure model
        iv. Take grant model
        v. sNET MLS model
        vi. An MLS policy model for networks – Vijay Varadharjan
        vii. Model for MLS in computer networks –Wen-Pai, Malar K. Sandaresthan
        viii. MLS METEOR model –Kang, NRL
        ix. An executive model for MLS workflows
        x. KSOS (Kernalized Secure Operating System)
        xi. Andre.
    b. Nei.
    c. Vet ikke.

    Eventuelt HVORFOR betegnes modellen som bedre enn andre.

    Hva karakteriserer en god modell/arkitektur/strategi?

    Finnes det fellestrekk mellom de gode modellene/arkitekturene/strategiene?

Forsvaret har ofte strengere krav til sikkerhet enn andre organisasjoner/bedrifter, og må kanskje ta andre hensyn ved innføring av MLS, enn det andre må gjøre.

2. **Er det i Forsvarssammenheng noen modeller/arkitekturer/strategier som er mer aktuelle enn andre? Begrunnelse.**
    a. Ja:
        i. Bell-LaPadula
        ii. The domain model – DERA,UK
        iii. UCLA data secure model
        iv. Take grant model
        v. sNET MLS model
        vi. An MLS policy model for networks – Vijay Varadharjan
        vii. Model for MLS in computer networks –Wen-Pai, Malar K. Sandaresthan
        viii. MLS METEOR model –Kang, NRL
        ix. An executive model for MLS workflows
        x. KSOS (Kernalized Secure Operating System)
        xi. Andre.
    b. Nei.
    c. Vet ikke.

    Eventuelt hvorfor er denne/disse mer aktuelle enn de andre?

    Hvilke premisser ligger til grunn for å velge denne modellen/arkitekturen/strategien?

    Er det en mulig løsning å kombinere flere modeller?

Teorier omkring MLS har eksistert i mange år; vi har blant annet funnet modeller fra begynnelsen av åttitallet. Begrepet MLS er altså ikke noe nytt og revolusjonerende, men et godt innarbeidet uttrykk innen teknologien.

3. **Vet du om det finnes utelukkende teoretiske modeller/arkitekturer/strategier, eller om det er noen av de som er realisert og i bruk?**
    a. Noen av de er realisert og tatt i bruk:
        i. Bell-LaPadula
        ii. The domain model – DERA,UK
        iii. UCLA data secure model
        iv. Take grant model
        v. sNET MLS model
        vi. An MLS policy model for networks – Vijay Varadharjan
        vii. Model for MLS in computer networks –Wen-Pai, Malar K. Sandaresthan
        viii. MLS METEOR model –Kang, NRL
        ix. An executive model for MLS workflows
        x. KSOS (Kernalized Secure Operating System)
        xi. Andre.
    b. Det finnes kun teoretiske modeller/arkitekturer.

    I hvilken sammenheng har den/de har blitt brukt?
    Er den/de fortsatt i bruk? Hvis nei, hvorfor ikke?
    Hvilke erfaringer som er gjort med denne modellen?

NATO har en gruppe som jobber med MLS og hvordan det kan benyttes i forsvarssammenheng. I og med at det ikke finnes ferdige løsninger som per i dag er gode nok for Forsvaret og NATO, må det være noen som jobber med å videreutvikle løsninger for dette.

4. **Hvem jobber med den videre utviklingen av modeller/arkitekturer/strategier innen MLS?**
    a. NATO
    b. Department of Defence, USA
    c. IBM
    d. Andre

    Hva konkret gjør gruppen som jobber med MLS i NATO?
    Hvis det er sivile selskaper som jobber med å videreutvikle MLS-løsninger, er det med hensyn på bruk i forsvarssammenheng?
    Vet du om det er enkeltpersoner eller institusjoner som innehar svært gode kunnskaper om MLSD, og som jobber spesielt med dette?

Etter det vi kjenner til, er det en del brikker som mangler for å få til en fullverdig MLS-løsning for bruk i Forsvaret. Flere aktører jobber med å videreutvikle generelle løsninger for MLS, og noen ser sannsynligvis på løsninger for bruk i forsvarssammenheng.

5. **Hvordan er progresjonen i arbeidet? Forklar.**
    a. Stor.
    b. Liten.
    c. Vet ikke.

Hvis det er noen som jobber med dette, hvor langt har de kommet?
Har de utviklet testnett, eller er de bare på teoristadiet?
Hvilke deler av en eventuell løsning er det de jobber med?
Er det komponenter, mekanismer, modeller, arkitekturer, strategier, eller annet?

Del 3: Konsekvenser av innføring av et system som sammenkobler informasjon med ulik sikkerhetsgradering.

Det har blitt forespeilet at en innføring av MLS kan skje i løpet av de neste ti årene. Dette vil høyst sannsynlig føre til en del endringer både i organisasjonen som helhet og for hver enkelt ansatt. Det dreier seg om endringer i forhold til sikkerhet, rutiner, informasjonsflyt m.m.

1. **Hvilke konsekvenser tror du en innføring av MLS vil få for Forsvaret som organisasjon?**
    a. Positive:
        i. Bedre informasjonsflyt.
        ii. Større fleksibilitet.
        iii. Bedre reaksjonsevne.
        iv. Bedre sikkerhet.
    b. Negative:
        i. Dårligere sikkerhet.
        ii. Store utgifter ved innføring.
    c. Annet.

Vil det være forskjeller mellom konsekvenser for operative enheter i forhold til andre enheter?
For hvilke deler av Forsvaret vil konsekvensene bli mest synlige?

En eventuell innføring av MLS vil trolig oppleves forskjellig ettersom hvor man jobber, og hva man jobber med. Endringene og konsekvensene ved innføringen av et slikt system vil sannsynligvis variere ettersom hvilke arbeidsoppgaver den ansatte innehar.

2. Hvilke konsekvenser vil en innføring av MLS få for de ansatte?

a. Positive:
   i. Større fleksibilitet.
   ii. Større effektivitet.
   iii. Tilgang til informasjon hvor som helst og når som helst.
   iv. Rask informasjonsflyt og dermed raskere saksbehandling.
   v. Annet.

b. Negative:
   i. Dårligere brukervennlighet.
   ii. Annet.

Hva med operativt personell i forhold til andre ansatte?
Hvem vil merke størst konsekvenser? Positive eller negative?

Foreløpig finnes det ingen MLS-løsning som er moden for bruk i forsvarssammenheng. Sett at man ikke kommer fram til en tilfredsstillende løsning for innføring av MLS, det være seg på grunn av sikkerhet eller annet.

3. Hvilke konsekvenser vil det få for Forsvaret hvis det IKKE implementeres MLS?

a. Positivt:
   i. Bedre sikkerhet.
   ii. Sparte kostnader.
   iii. Annet.

b. Negativt:
   i. Lite fleksibilitet.
   ii. Liten effektivitet.
   iii. Treg informasjonsflyt og dermed sein saksbehandling.
   iv. Økte kostnader.
   v. Annet

c. Situasjonen vil forbli som i dag.

Hvilke deler vil lide mest på grunn av dette?
Vil dette gjøre Forsvaret til en organisasjon som ”ikke følger med i tiden”?
I takt med at den teknologiske utviklingen fortsetter, vil Forsvaret lide av dette?
Hvor lenge er det sannsynlig at man forsetter å bruke ressurser på å utvikle en god nok MLS-løsning for bruk i forsvarssammenheng?

Det kan tenkes at innføring av MLS ikke blir noen realitet. Man har et system i dag, og det snakkes også om å innføre MSL som en midlertidig løsning før MLS.

4. Finnes det noe alternativ til MLS?

Er det et alternativ å fortsette som i dag?
Er MSL en mulig løsning?
Hva med andre løsninger?
Er det noen som jobber med dette, eller er MLS det eneste man har i tankene?

Tilleggsspørsmål:

Vi har forstått det slik at MLS er den løsningen Forsvaret ønsker seg. Det finnes imidlertid ingen konkrete løsninger som er gode nok per i dag. Det er flere momenter som gjør at dagens MLS-løsninger ikke kan brukes.

1. Hva er det som er til størst hinder for en innføring av MLS i Forsvarssammenheng?

a. Gjeldende sikkerhetsbestemmelser.
b. Modellene er for dårlige.
c. Arkitekturene er for dårlige.
d. Strategiene er for dårlige.
e. Teknologien er ikke god nok.
f. For store kostnader vedrørende implementering av MLS.
g. Det finnes ingen hindringer.

Eventuelt hvilke deler av modellene/arkitekturene/strategiene er ikke gode nok?
Er hindringene de samme for alle nasjoner?

Vi har sett ulike årstall for når MLS er tenkt innført i Forsvaret. Noen steder står det konkrete årstall som 2014, enkelte personer har ikke tro på innføring av MLS i det hele tatt.

2. Har du noen formening om når Forsvaret kan ta i bruk MLS?

h. Ja:
    i. I 2014.
    ii. Det vil aldri bli tatt i bruk.
    iii. Annet.
i. Nei.

Eventuelt hvor lang tid vil det ta fra man har en konkret løsning, til MLS er ferdig implementert?

Vedlegg B: Resultater fra kvalitativ undersøkelse 1.

NB! Resultatene er gitt til denne oppgaven og kan ikke brukes av andre, uten intervjuobjektenes samtykke!

Innledende spørsmål

Navn	Stilling	Kommentar
Øyvind Nyquist	Prosjektsikkerhetsleder FISBasis og Systemforvalter Tonivå og Sikkerhet.	
Øyvind Hvinden	Senior Principal Engineer Lead, C4ISR Infrastructure Development Norwegian Defence Logistics Organization/CIS Division Systems Solutions/Operational Systems Branch.	
Håkon Liberg	Senior Security Consultant IBM - Integrated Technology Services.	Konsulent i Program Golf, men har uttalt seg som privatperson i undersøkelsen.
Nicolay Nakstad	Ansatt i Sentral Sikkerhetsgruppe, Program Golf.	
Jon Ølnes	Senior Researcher, DNV Research.	Tidligere ansatt i IBM, og konsulent i Program Golf.

Delproblem 1

Spørsmål 1:
Er det de gjeldende sikkerhetsbetemmelser som hindrer Forsvaret i å ta i bruk MLS?

Ø. Nyquist	Spørsmålet er ikke mulig å besvare med ja eller nei. Implementering, drift og bruk av MLS systemer forutsetter at noen, fortrinnsvis sikkerhetsmyndigheten, kan definere hva MLS innebærer for en stor "enterprise-løsning" som FISBasis. I denne sammenheng har FISBasis inkludert de funksjonelle produksjonssystemene. Dette er ingen liten eller enkel oppgave. Integrasjon mellom plattform (Windows – server, katalog, klientprogramvare, etc), og de funksjonelle systemene er avgjørende for en slik avgrensning/definisjon. Svaret på spørsmålet tenderer til et ja – derom man trekker fram grad av tillit som må etableres gjennom evaluering og sertifisering. Eller svaret er så enkelt at det ikke finnes noen MLS-systemer å benytte! Tillitsnivået som må til for å definere et MLS-system. Ser vanskeligheter med å gjennomføre fullstendige MLS-løsninger. Ser heller muligheter for mer delvise MLS-løsninger. Hvilke deler av SAP må man ha tillitt til for at det skal bli et SAP-MLS-system? (SAPDEIG). Kravene til tiltro er til hinder, og det skremmer vekk industrien. Forsvaret og NATO har ikke stor nok markedskraft til å påvirke.
Ø. Hvinden	Nei.
H. Liberg	Ja, de formelle kravene fra NSM er altfor strenge. Dette går på det prinsipielle. NSM sier at dette er noe de ikke vil diskutere. Per i dag er det ikke lov å sammenkoble systemer med forskjellig gradering. Når NSM ser svart/hvitt på det, er det umulig for oss som leverandør å diskutere mulige løsninger.
N. Nakstad	Det er flere ting som hindrer dette: 1. Merking av dataelementer (tagging). 2. Det at systemene ikke er klare, teknologien er for dårlig. 3. Regelverket. Det er liten vits i å utvikle teknologien videre før regelverket åpner for en slik løsning. Foreløpig er regelverket åpent for to nivåer. En kan sitte på en gradert plattform, og ved bruk av en Citrix Ica-klient kan en få tilgang til en annen, men man kan ikke sitte på flere Citrix-Ica-klienter. *Tagging: Objekter som pakkes inn i et tagget skall. Dersom skallet brytes → ny gradering.* *Labelling: Dataene har et felt som er låst for en liten sak. Objekter har flere slike felter. Tilnærming mot MLS.* *Det er IKKE ønskelig å flytte HEMMELIG informasjon ned på BEGRENSET, men*

	BEGRENSET-HEMMELIG ned på BEGRENSET.
J. Ølnes	Til dels, ja. NATO-krav ser ut til å blokkere for integrasjon mellom systemer på HEMMELIG og systemer på BEGRENSET, når systemene på BEGRENSET samtidig har integrasjon mot ugradert nivå. Men disse kravene er antagelig i endring, og er nødt til å bli endret dersom en skal realisere et nettverksbasert forsvar. Norsk lovgivning/forskrifter mener jeg ikke skal være til hinder, men NSM har hatt en meget streng holdning til betingelser for å tillate slik integrasjon – på grensen til blokkerende.

Spørsmål 2:
Eventuelt hvilke sikkerhetskrav er de mest avgjørende?

Ø. Nyquist	Henger sammen med redegjørelsen foran. Integrasjon /grensesnitt problematikk gjør det nærmest umulig å definere noe som MLS med mindre systemet har en holistisk arkitektur: det vil si at plattform og funksjonelle systemer er ett og samme. Evaluerings- og sertifiseringskravene er altfor høye. Kravet er ofte at alle underliggende mekanismer er sertifiserte sammen med et eventuelt system, for å få noe godkjent.
Ø. Hvinden	• Krav til tiltro (assurance). Dette er det tøffeste kravet innen MLS. Tiltro til at softwaren er god nok. • Lover som forbyr SECRET-system å kobles mot Internett, har store konsekvenser for muligheten for informasjonsutveksling med Internett eller systemer tilknyttet Internett. Alle ansatte i Forsvaret har tonivå Internett-løsning fra Forsvarets BEGRENSEDE systemløsning (FISBasis). Og det betyr at Forsvaret ikke kan MLS-sammenkoble sine hovedsystemer på BEGRENSET og SECRET/HEMMELIG nivå med store konsekvenser for aktuell informasjonsutveksling. • NATO-policy gjelder for Forsvarets systemer fordi NATO-inforamsjon håndteres i nesten alle av dem.. NATO-policy er nå noe myket opp med henblikk på knyting mot Internett. Det finnes enveisløsninger med informasjonsflyt nedenfra og opp, med høy tiltro. Det er imidlertid viktig også å få til informasjonsflyt ovenfra og ned. Beslutninger tas høyt oppe, og må ut igjen til personer via lavgradert nivå. Det er store mengder informasjonsflyt nedenfra og opp, eksempelvis værdata, antivirusfiler fra Internett etc. Noe informasjon går ovenfra og ned, og det er dette som er den største utfordringen.
H. Liberg	Sikkerhetsloven med forskrifter og veiledninger.
N. Nakstad	Nato-krav, Infosec nummer 33.
J. Ølnes	NATO-krav ser ut til å være styrende på linje med nasjonal lovgivning. NSM er ansvarlig for sikkerhetsgodkjenning og kan blokkere det de ikke finner tilfredsstillende.

Spørsmål 3:
Hvilken betydning vil det ha dersom nåværende sikkerhetskrav senkes?

Ø. Nyquist	Igjen, for MLS er dette irrelevant. Krav til MLS systemer må gjerne bestå. Diskusjonen og utviklingen bør derimot dreies mer mot oppnåelige løsninger, basert på risikovurderinger, der konklusjonene for hva som er nødvendig og tilstrekkelig sikkerhet er fokus. Dersom dette resulterer i at man på enkelte funksjonelle elementer må ha stor grad av tillit (evaluerte og sertifiserte produkter), så kan det aksepteres. Det ville sannsynligvis blitt enklere å lagre strukturerte data i databaser i MLS, mens ustrukturerte data ville blitt mye verre.
Ø. Hvinden	• Større fare for kompromittering av graderte data. • Tiltroen til de tilgjengelige MLS-produktene er ikke god nok til å møte HEMMELIG/BEGRENSET mot BEGRENSET/Internett.
H. Liberg	• Det vil åpne mulighetene for å innføre MLS. • Det vil gjøre det mulig å diskutere hvilke systemer som fyller de nye kravene. • Hvis Forsvaret senker kravene kan systemene fra IBM vurderes, spesielt med tanke på et nettverksbasert forsvar (NbF). Et NbF er ikke mulig med dagens krav. • Angående sikkerhet, så dreier dette seg om en gråsone. Per definisjon vil sikkerheten bli dårligere, men ikke så avgjørende at hele løsningen settes på spill. • NSM er erfaringsmessig ute etter det beste og vil at alle mulige krav skal tilfredstilles, noe som hindrer implementering av gode og rimelige løsninger. Noe som gjør at det er vanskelig å nå en 100 % løsning, er at de ofte sitter med en 90 % løsning og diskuterer

	hvordan i alle dager de skal greie å tilfredsstille de siste 10 %. Mener at NSM skyter seg litt i beinet.
N. Nakstad	Forsvaret vil bli mindre sikkert. Slik det er i dag er det umulig å angripe HEMMELIG fra ugradert.
J. Ølnes	Det spørs hva en mener med sikkerhetskrav. En trenger et langt sterkere fokus på tilgjengelighet (og integritet) framfor konfidensialitet. Hva er risikoen dersom informasjon ikke er tilgjengelig vs. risikoen dersom informasjonen kommer uvedkommende i hende? "Senke kravene" er feil formulering, men senke krav til konfidensialitet til fordel for andre sikkerhetskrav. Dersom en skal realisere nettverksbasert forsvar, er en helt nødt til å se på risiko i en slik utvidet sammenheng, ikke bare på konfidensialitet.

Spørsmål 4:
Jobbes det med å endre disse kravene?

Ø. Nyquist	Nei, ikke det jeg vet. Ikke ser jeg noen hensikt i det heller, ref det jeg har redegjort for i foregående punkt.
Ø. Hvinden	Nei. Her i Norge er det NSM som stiller kravene. Arbeidsgrupper i Nato C3-board, Subcommitees 4, ser på sammenkoblinger av systemer. Her har NSM en representant. Landene kommer sammen og setter regelene, de som er mest forsiktige av landene på sikkerhet, får som oftest viljen sin. Her er det de strengeste som styrer. Holdningene er forskjellige fra land til land. Det som vedtas nedfelles i formelle dokumenter. Det kom for ikke så lenge siden, en Nato-policy som åpnet for bruk av diode med enveis overføring. tidligere var det absolutt ikke lov å sammenkoble systemer mot Internett. Norge er forpliktet å signere et dokument som het CM-55-15; alle land signerer på dette. Går på informasjonssikkerhet, fysisk sikkerhet, dokument sikkerhet. NSM MÅ følge Nato i henhold til internasjonale sikkerhetsbestemmelser. Dette henger nøye sammen med høygradert nasjonalt nivå da dette ofte er koblet mot NATO. NSM trenger ikke følge NATO-bestemmelsene for nasjonalt graderte systemer, så lenge disse ikke er koblet opp mot NATO.
H. Liberg	Ikke meg bekjent. Man bør muligens framprovosere flere diskusjoner mot NSM og utfordre lovverket i forbindelse med LP2 i motsetning til LP1.
N. Nakstad	Veldig få vet hva som egentlig skjer med dette. NSM er representert i disse fora og påvirker kanskje i Nato, FSA rådgiver departementet her, det vil si folk som sitter i Nato. Det er et arbeid pågående som skal spisse ordlyden slik at misforståelsene med ordbruk forsvinner i NATO-sammenheng, noe som kan gi en åpning til å knytte systemer sammen.
J. Ølnes	Dette er ting vi har tatt opp fra/i Golf FP2. Se Vedlegg 1 til leveransen på Sikkerhetskonsept for LP2 (Sikkerhetsutfordringer i LP2). Det foreslås å legge mye større vekt på risikovurderinger og praktiske løsninger, mindre vekt på "absolutte" krav.

Spørsmål 5:
Er det nødvendig å endre sikkerhetskravene for å implementere MLS i Forsvaret?

Ø. Nyquist	Ikke besvart! Spørsmålet ikke stilt!
Ø. Hvinden	Nei. Å endre sikkerhetskravene er ikke veien å gå for å innføre MLS. Det å endre kravene så mye er urealistisk.
H. Liberg	Ja, det er helt nødvendig. NSM sier det er umulig med MLS og dagens sikkerhetskrav med tanke på at MLS dreier seg om sammenkobling av systemer med forskjellig gradering. Det er ikke lov til å sammenkoble systemer på HEMMELIG med lavere graderte systemer i dag.
N. Nakstad	Ja, det er helt nødvendig. MLS innebærer å knytte to ting sammen, og dette er ikke lov per i dag.
J. Ølnes	MLS er for så vidt i bruk, men bare for små komponenter. For eksempel er vel overføringssonen for FISBasis 2-nivåløsning å betrakte som MLS, og det samme gjelder Forsvarets meldingssystem. "Diodeløsninger" for overføring fra lavgraderte systemer til

	høygraderte, er vel også innen denne kategorien. Til dels er det snakk om å tilpasse krav, men det største problemet er at sertifisering (CC EAL4 eller høyere) er meget upraktisk for annet enn små systemer, og spesielt upraktisk der en har systemer som oppdateres jevnlig (ikke statiske).

Delproblem 2

Spørsmål 1:
Det finnes mange teoretiske modeller/ arkitekturer/ strategier innen MLS. Er et noen av disse som betegnes som bedre enn andre? Begrunnelse.

Ø. Nyquist	Partisjonert operasjonsmåte, ikke MLS, er det det snakkes om. Send-til-meny, dialogboks med forespørsel om release-streng. Kan sende fra høyere til lavere gradering. Blir innført for alle nå. Noe MLS, men ikke fullstendig. Manuell angivelse (kode). Veien å gå til MLS er lenger å gå enn til MSL. Avhengig av noe "MLS Light" for å sette release-strenger. For å sammenkoble/behandle NATO-systemer er man avhengig av å følge deres sikkerhetskrav. Eksempel: Overføring via VPN/PKI, eventuelt primærforsikring. Ser til at riktig release-streng sendes videre. Dette er ikke MLS, men likner kanskje med tagging etc. Dette forutsetter endring av policy. NB! Veiledninger er ikke lov! FIF har også behov for å knytte sammen systemer, HEMMELIG og Internett etc.
Ø. Hvinden	Kjenner best Orange Book-modellen (Trusted Computing Base). Bell-LaPadula ligger for grunn til Orange Book.
H. Liberg	Det er etablert en gruppe, Trusted Computing Group (IBM, Microsoft etc.).
N. Nakstad	Blankt!
J. Ølnes	Ingen sterke synspunkter her i farta.

Spørsmål 2:
Er det i Forsvarssammenheng, noen modeller/arkitekturer/strategier som er mer aktuelle enn andre? Begrunnelse.

Ø. Nyquist	• Toveis utveksling av data bygget på nåværende regelverk. • Utvikling, promotering og drifting er svært kostbart, også å forvalte. Vanskelig å se for seg hvem som kan koste et MLS-system. • Fokus er sammenkobling mellom ugradert og BEGRENSET. Man stanger hodet i veggen ved sammenknytting mellom HEMMELIG og BEGRENSET.
Ø. Hvinden	• Partisjonert fellesnivå (NSM som har kalt denne for dette): - Flere domener på samme nivå - Flere brukere - Hver operasjon, for eksempel KFOR, SFOR og ISAF, har et eget system. Det samme er gjort nasjonalt: NS partisjon, rik informasjonsutveksling. - Mange systemer på høyt nivå som er sammenkoblet til en viss grad → partisjonert fellesnivå • Tonivåløsning: - FIS/BASIS - MLS med lite spenn uten bruk av MLS-komponenter - Ugradert og BEGRENSET • Diodeløsning (enveis informasjonsflyt): - HP/Tenix datadiode (datapumpe), et australsk produkt, www.Tenix.au. - Det jobbes med typegodkjenning mot NSM. - Pumper kun opp. • Applikasjonssikkerhet (trusted plug-in): - Metode som brukes av flere land. - Sikkerhetsmerking/ digitale signaturer nyttes for å sikre/beskytte data. - Kryptering på applikasjonsnivå, dette er imidlertid vanskelig å få sikkert. - C2 with labelling, datanivå med sikkerhetsmerking. - Tagging av informasjon som blir signert og sendt. • Avgrenset MLS-funksjonalitet:

	- En eller flere applikasjoner forsterkes og samarbeider med en guard mellom to systemer. - Nedgradering: MLS-boks på grensesnittet. En person merker om informasjonen. Vedkommende må være et orakel for å klare dette (review and release), så dette fungerer ikke særlig godt i virkeligheten. Det er nok bedre med merking fra utsteder, slik at nedgraderingen kan gå automatisk. Utsteder får da sette på sikkerhetsmerking.
H. Liberg	Blankt!
N. Nakstad	1. Har sett en lysbildepresentasjon med en gammel løsning fra Oracle. Helt uanvendbar, men fullstendig MLS-løsning. Lukket system, ingen forbindelse ut. 2. Sun Solaris: Gammel, gitt opp, produseres ikke lenger.
J. Ølnes	I Golf FP2 skisserte vi integrasjonsstrategier basert på Web Services og sikkerhetsgatewayer. Poenget er en sterk soneinndeling og sterk kontroll på trafikk mellom soner (enten disse er på forskjellige graderingsnivåer eller innen samme graderingsnivå). Strategien er da ikke store MLS-systemer, men separate systemer og "MLS-integrasjonsløsninger". I noen dokumenter er dette omtalt som MSL (Multi System Level). Jeg/vi i FP2 har liten tro på at store systemer på noen praktisk måte kan være MLS (bl.a. pga. sertifiseringer). Derfor separate systemer og systemintegrasjon, der deler av integrasjonsløsningene (sikkerhetsgatewayer) må være MLS. Dette stiller også krav til intern sikkerhet i hver sone/system, men i hovedsak kan disse kravene være iht. det som gjelder for det aktuelle graderingsnivået.

Spørsmål 3:
Vet du om det finnes utelukkende teoretiske modeller/arkitekturer/ strategier, eller om det er noen av de som er realisert og i bruk?

Ø. Nyquist	Mail Gatewayen til nordisS, og meldingstjenesten.
Ø. Hvinden	CMW, compartment workstations → MLS for 10 år siden på FLO/IKT Til størst hinder er at det er ofte litt gammeldags teknologi → Unix
H. Liberg	Realiserte MLS-systemer: • Det som IBM solgte til et farmasøytisk firma. Solgt som et MLS-system og er i bruk. Skal finne bakgrunnsinformasjon og sende. • I Golf har det blitt diskutert en diode-løsning. • NATO: I forbindelse med fly. Nato sender informasjon om hvilke NATO-fly som skal fly når og hvor, til sivil luftfart. Går fra HEMMELIG til ugradert system. Christophersen vet mer om denne løsningen.
N. Nakstad	Blankt!
J. Ølnes	Ja, det finnes ting som er i bruk, men erfaringer er vel temmelig blandet. Igjen: Dette har med nødvendige sertifiseringer å gjøre, og at en ender opp med statiske systemer med meget kompliserte rutiner for oppgraderinger (og endog feilrettinger). Brukervennligheten blir lav. Også i Norge har en sett på "Compartment mode workstation", men jeg kjenner ikke til erfaringene med dette. Det mest aktuelle er mindre tekniske komponenter for integrasjon mellom systemer på ulike graderingsnivåer.

Spørsmål 4:
Hvem jobber med den videre utviklingen av modeller/arkitekturer/ strategier innen MLS?

Ø. Nyquist	Program Golf gjør det, men kommer ikke i mål...for de jobber ikke med MLS…?? (www.commoncriteria.com) → som regel spesialiserte løsninger som er evaluert.
Ø. Hvinden	Datamaskin/operativsystemleverandører, for eksempel SUN Trusted Solaris. Det amerikanse forsvaret i samarbeid med dataindustrien i USA.
H. Liberg	Trusted Computing Group. Usikkert om dette er MLS eller ikke. Jeg antar videre at det foregår forskning på området blant forsvarsleverandører.
N. Nakstad	SAP DEIG (Defence Interest Group). Fora for Forsvaret jobber med dette. På grunn av at SAP er valgt som system, jobbes det videre med SAP-løsninger. En interessegruppe med representanter fra blant annet USA, Tyskland, Danmark, Norge og Tyrkia har sett på kravspesifikasjoner. Det er et problem med labelling, noe som SAP ikke støtter i dag, men SAP har sagt at de vil ordne dette. Gruppen har kommet fram til en del interessante ting: matriser med hensyn til roller, lokasjon og rettigheter. Matrisen ble som en CUBRIX-kube

	(Lattice?), ikke todimensjonal. Flere-login. Kan spørre Ø. Christoffersen ved NSM om noe publisert materiale.
J. Ølnes	Dette har jeg forholdsvis lite kjennskap til (jobbet for en bestemt leverandør). For SAP finnes det DEIG (Defence Interest Group) som ser på – sammen med SAP AG – MLS-versjoner av SAP. Dette har jeg personlig liten tro på, men det er et aktivt arbeid. SAP kan realisere mye av den ønskede funksjonaliteten, men det vil være umulig å sertifisere SAP til EAL4 el.

Spørsmål 5:
Hvordan er progresjonen i arbeidet? Forklar.

Ø. Nyquist	Hinder for innføring: Tillitsnivå
Ø. Hvinden	Blankt!
H. Liberg	IBM har teorier for hvordan det burde være, men formelle krav setter en stopper for dette.
N. Nakstad	Bare SAP vet om mulig dette.
J. Ølnes	Det vi foreslo fra Golf FP2, er å se på systemintegrasjon mellom systemer på ulike graderingsnivåer, men holde systemene på ett nivå (altså ikke MLS-systemer). "En fullverdig MLS-løsning" vil da etter mitt syn bestå av en fullverdig integrasjonsløsning etter disse retningslinjene. Se vedlegg 2 og 3 til FP2s leveranse på Sikkerhetskonsept for LP2 for mer om dette. Progresjon i arbeidet vet jeg for lite om til å kunne uttale meg.

Delproblem 3

Spørsmål 1:
Hvilke konsekvenser tror du en innføring av MLS vil få for Forsvaret som organisasjon?

Ø. Nyquist	Igjen: Bruken av begrepet MLS er unyansert og ukorrekt. Jeg har ikke tro på MLS for store løsninger som FISBasis med applikasjoner, driftsløsninger, etc. System high, eller mer korrekt fellesnivå operasjonsmåte er mer enn tilstrekkelig sikkert på for eksempel BEGRENSET graderingsnivå. Det det handler om er å kunne utveksle data mellom graderingsnivåer på en mer fleksibel og effektiv måte. For at dette skal kunne la seg gjøre må det sannsynligvis utvikles/videreutvikles en del funksjonelle elementer, både i applikasjonssystemer og infrastruktur, som har elementer som kan likne på MLS, herunder merking av objekter (data), tjenester som leser disse merkingene og agerer på bakgrunn av dette. Tradisjonell MLS tankegang i denne sammenheng betyr at disse funksjonelle elementene må underlegges ekstreme tillitskrav – evaluering og sertifisering i henhold til CC, ITSEC eller TCSEC, som industrien ikke er villige til å finansiere. Hvis det hadde latt seg gjennomføre, så hadde en innføring av MLS vært veldig positivt for Forsvaret. Kjempefordel med tilgang til Internett og ulikt graderte data på ett og samme system.
Ø. Hvinden	• Bedre informasjonsflyt mellom det høygraderte domenet og det BEGRENSEDE domenet. • Dårligere funksjonalitet og fleksibilitet. • Det vil kreve veldig nøye sikkerhetsmerking av informasjon, hvilket vil sette store krav til brukerne. Er man logget inn på HEMMELIG blir informasjonen HEMMELIG, og denne må derfor merkes slik at den kan nedgraderes. Det er ikke mulig å være logget på to eller flere nivåer samtidig. • Med et ideelt produkt og god opplæring blant brukerne, kunne MLS blitt mulig.
H. Liberg	1. I krig: • Informasjonsoverlegenhet, mindre tap for en selv. • Fare for at fienden kan komme seg inn på systemet og få tak i sensitiv informasjon. 2. I fredstid: • Bedre informasjonsflyt. Innkjøp av utstyr har tidligere blitt gjort på feil grunnlag. For eksempel innkjøp av utstyr som allerede eksisterer. • Personellsikkerhetsbiten blir enda viktigere. Hvem som får tilgang til hva. Kinkig situasjon.

	NB! Informasjonsoverlegenhet overgår mulig lekkasje av informasjon. Kvaliteten i et MLS-system vil være bedre enn dagens hyllevare (Windows etc.). Årsak: Oppbygningen av systemet er veldig metodisk og strukturert
N. Nakstad	• Må gjøres noe med (NSM). • Informasjonsoverlegenhet. • Økonomisk besparende rent lagringsmessig. • Litt avhengig av hvilke løsninger som en kommer med. Kanskje bedre sikkerhet. Rolletildelinger og personlig ansvar; her kreves det en stor oppvask. Hvis ikke vil sikkerheten bli dårligere. • En innføring vil kreve store utgifter. Annet: • Graderingsnivåer har levetid (eks 5 år). • Informasjonsdatabasen blir veldig stor, kanskje med informasjon som strengt att ikke burde vært der. Tidsperspektiv for nedgradering.
J. Ølnes	Først: En skal kople sammen SYSTEMER på ulike graderingsnivåer, ikke INFORMASJON. Dersom en integrerer et system på HEMMELIG med et system på BEGRENSET, må en integrasjonsløsning sikre at informasjon håndteres i henhold til. graderingsnivå. Det vil si: • Systemet på BEGRENSET skal ikke ha høyere gradert informasjon, og informasjon skal derfor kunne flyte "opp" (men iht. need-to-know prinsippet). • Systemet på HEMMELIG kan holde informasjon som er gradert BEGRENSET eller er ugradert, og kun denne informasjonen kan sendes til systemet på BEGRENSET!! • Systemet på HEMMELIG vil holde informasjon gradert HEMMELIG, og denne skal under ingen omstendighet sendes til et lavere gradert system. Som sagt tror jeg at de operative systemene ("de med brukere") vil være på ett graderingsnivå og ikke MLS. Effekten for brukerne tror jeg derfor ikke vil være stor, men en trenger nok en økt bevissthet på hva slags informasjon en sender til andre systemer (der dette er kontrollert av brukerne). For Forsvaret som organisasjon er effektene rimelig bra beskrevet i "Nettverksbasert Forsvar" og "Arkitektur for Program Golf" (ikke helt nøyaktige dokumenttitler).

Spørsmål 2:
Hvilke konsekvenser vil en innføring av MLS få for de ansatte?

Ø. Nyquist	Fordeler: - Hverdagen for brukere på alle nivåer (saksbehandler, leder, controller, etc.) og innen alle funksjonsområder vil få bedre systemstøtte for sine arbeidsprosesser. Kjempefordel med flere graderinger på samme system. - Ville forenkle situasjonen for alle, og vil sannsynligvis ikke bli verre å administrere enn i dag. Ulemper: - IKT-systemene blir noe mer komplekse, det kreves mer med hensyn til drift, konfigurasjonsstyring, change, videreutvikling, etc. Imidlertid tror jeg gevinstene vil bli forholdsmessig større enn kostnadene. - Problemer med riktig prioritering mtp....? - Verre å administrere. - Definering av tabeller og sammenstillinger som gjør at ting blir gradert.
Ø. Hvinden	BEGRENSET informasjon kan bli tilgjengeliggjort på HEMMELIG system for operativ bruk: personell, økonomi, materiell Informasjon fra HEMMELIG system relatert til for eksempel operative materiellproblemer kan overføres til BEGRENSET operativt støttesystem hvor materiellhåndtering som logistikk og bestillinger foregår.
H. Liberg	• Tilgang til informasjon hvor som helst og når som helst. • Tilgang til mer data. • Bedre brukervennlighet. Høy tilgjengelighet, ting på skinner.. • Burde være flere og bedre kontroller på autorisasjon (tilgang til systemer) enn det som er i dag. Argumenter for HVORFOR noen trenger tilgang. I dag er det forholdsvis enkelt å få tilgang. Tjenestemessigbehov bør være klare og styrende, hvorfor trenger du

	tilgang til det.
N. Nakstad	Det er de operative som vil merke det mest, det vil bli best for dem. Tilgang til alt fra et sted, mindre å holde styr på. Samtidig vil det kreve ytterligere omstilling.
J. Ølnes	Se forrige spørsmål. Effekten for brukerne KAN IKKE være stor – da vil neppe dette være sikkert nok. Hold "systemer med brukere" innen ett graderingsnivå!

Spørsmål 3:
Hvilke konsekvenser vil det få for Forsvaret hvis det IKKE implementeres MLS?

Ø. Nyquist	• Må opprettholde relativt tungvinde systemer med overføring mellom nivåer. • Mer Personell og kostnader i forbindelse med drift hvis ikke det blir innført.
Ø. Hvinden	Da får man ikke tjenester som angitt ovenfor realisert på en effektiv måte. Metoder som luftgap for overføring av informasjon må benyttes som er langsommere og krever mer bemanning.
H. Liberg	• Dagens formelle/teoretiske krav til MLS er sinnsykt avansert og kostdrivende. • Dagens dobbeltløsning er tungrodd. • Dobbel lagring av informasjon. • Oppdateringsproblematikken vil være tilstede. Forskjellig informasjon i ulike systemer vedrørende materiell og annet. Hvilken informasjon skal man stole på i en krigssituasjon? Er informasjonskvaliteten høyre på HEMMELIG eller høyere på BEGRENSET? Eller skal en stole på erfaring?
N. Nakstad	• Det vil fortsette som dagens situasjon. Det fungerer, til en viss grad. • Ellers er det en fare for et alt graderes, det vil si at alt settes som BEGRENSET, slik at man får all informasjon inn på samme plattform. Dette er svært uheldig med tanke på at noe informasjon er KONFIDENSIELL og HEMMELIG.
J. Ølnes	Manglende systemintegrasjon mellom systemer på ulike graderingsnivåer (slik vi har beskrevet i Sikkerhetskonsept for LP2) vil være en kritisk mangel. En vil ikke kunne realisere et nettverksbasert forsvar, og en vil ikke kunne dele informasjon som forutsatt. Jeg legger til grunn at en ikke vil ha MLS-systemer annet enn for integrasjonsløsningene.

Spørsmål 4:
Finnes det noe alternativ til MLS?

Ø. Nyquist	• Et vist innslag av MLS der en merker objektene. • Når det gjelder FISBasis med 300 applikasjoner, så kan jeg ikke forestille meg at dette lar seg gjennomføre med MLS. • Hvis MLS: Gradering vil vises i det vinduet som er oppe. Anser dette som en ulempe for de ansatte. Må tenke over på forhånd hvilken gradering det en skal produsere… • I dag har vi: BEGRENSET-HEMMELIG: enveis Ugradert-BEGRENSET: begge veier (tonivå)
Ø. Hvinden	Alternativet er bruk av luftgap mellom systemene og manuell løfting/flytting av informasjons.
H. Liberg	• Diodeløsning. • Noe informasjon fra et sted osv. (det vil si en rekke forskjellige systemer) • Reell fare: Ting samles i ett system, eksempelvis FIF. Dette er ikke MLS, men kan bli brukt som det på område BEGRENSET. Aggregering av data gjør at det i trolig er over BEGRENSET. Dette vil gi økt fare for lekkasje. Får ikke den kontrollen over autorisasjoner som en burde ha.
N. Nakstad	MSL: Større samhandling mellom systemene. Jeg tror at vi beveger oss i denne retningen. MLS er ikke etterspurt og ingen forventer det. Golf tenker økonomi. Å innføre noe som ikke er etterspurt er dømt til å mislykkes. FISBasis snuser på MSL, Citrix-tilgang til andre plattformer, men må gjøre manuelle steg for å flytte informasjonen.
J. Ølnes	Det meste av det jeg snakker om i mine svar, er MSL. Jeg tror dette også er den langsiktige løsningen (integrasjon mellom systemer på ulike graderingsnivåer), og jeg har ikke tro på at større, kompliserte systemer kan oppnå godkjenning (fra NSM) som MLS-systemer – heller ikke på sikt.

Vedlegg C: Spørreskjema til Kvalitativ undersøkelse 2

Spørreskjema

Svar ved å sette kryss i firkantene. Utdyp gjerne svarene i merknadsfeltet.

Definisjon på MLS
MLS beskriver en arkitektur som lar data med forskjellige klassifiseringsnivåer oppholde seg på samme system eller nettverk. I et MLS system eller nettverk, skiller systemet de forskjellige dataene ved bruk av etiketter.

1. **Navn: _____**

2. **Stilling og arbeidssted: _____**

3. **Hvilke graderingsnivåer jobber du på?**
   - ☐ Ugradert
   - ☐ BEGRENSET
   - ☐ HEMMELIG
   - ☐ NATO UNRESTRICTED
   - ☐ NATO RESTRICTED
   - ☐ NATO CONFIDENTIAL
   - ☐ NATO SECRET
   - ☐ Annet:

Merknad: _____

_____

_____

4. **Hvor lenge har du jobbet med de ulike nivåene?**
   - ☐ 0-1 år
   - ☐ 2-3 år
   - ☐ Over 4 år

Merknad: _____

_____

_____

5. **Hvilke(t) nivå(er) jobber du på til daglig?**
   - □ Ugradert
   - □ BEGRENSET
   - □ HEMMELIG
   - □ NATO UNRESTRICTED
   - □ NATO RESTRICTED
   - □ NATO CONFIDENTIAL
   - □ NATO SECRET
   - □ Annet: _____

Merknad: _____

_____

_____

6. **Hvor ofte skifter du mellom å jobbe på de ulike nivåene?**
   - □ 1-3 ganger dagelig
   - □ 4-10 ganger dagelig
   - □ Over 10 ganger dagelig

Merknad: _____

_____

_____

7. **Hvor mange forskjellige brukerstasjoner bruker du på en gjennomsnittlig arbeidsdag?**
   - □ 1
   - □ 2
   - □ 3
   - □ 4 eller mer

Merknad: _____

_____

_____

8. Hvor ofte skifter du brukerstasjoner for å komme inn på forskjellige nivåer?

- 1-3 ganger daglig
- 4-10 ganger daglig
- Over 10 ganger daglig

Merknad: _____

_____

_____

9. Hvordan er brukervennligheten med dagens systemer/informasjonsflyt? (Svar gjerne med utfyllende kommentar.)

- Lite god
- God
- Svært god

Merknad:_____

_____

_____

10. Føler du at dagens system er tungvindt på noen måte? Hvis Ja, utdyp i merknad.

- Ja
- Nei
- Vet ikke

Merknad:_____

_____

_____

11. Hvor mye av informasjon på de HEMMELIGE nettene kunne etter din mening, ha vært nedgradert?

- 0-30 %
- 40-60 %
- 70-90 %
- Over 90 %

Merknad: _____

_____

_____

12. Finnes det mye lik informasjon på de ulike nettene?

- over 90 % av informasjonen er dupleks
- 70-90 % er dupleks informasjon
- 40-60 % er dupleks informasjon
- 10-30 % er dupleks informasjon
- Det er nesten ingen dupleks informasjon

Merknad: _____

_____

_____

13. Tror du at mye av informasjonen på det HEMMELIGE nettet, vil bli nedgradert til BEGRENSET, hvis Forsvaret innfører MLS?

- over 90 % av informasjonen vil bli nedgradert
- 70-90 % av informasjonen vil bli nedgradert
- 40-60 % av informasjonen vil bli nedgradert
- 0-30 % av informasjonen vil bli nedgradert
- Det er nesten ingen dupleks informasjon

Merknad: _____

_____

_____

14. Hvor lang tid tror du det vil ta før et MLS-system innføres i Forsvaret?

- 0-1 år
- 2-5 år
- 6-10 år
- Mer enn 10 år
- Aldri

Merknad: _____

_____

_____

15. Vil MLS gjøre hverdagen enklere for deg? Hvis Ja, utdyp hvordan i merknad.

- Ja
- Nei
- Vet ikke

Merknad: _____

_____

_____

16. Vil MLS forenkle informasjonsflyten? Hvis ja, utdyp i merknad.

- Ja
- Nei
- Vet ikke

Merknad: _____

_____

_____

17. Er det etter din mening noen spesielle prosesser som vil bli enklere ved en eventuell innføring av MLS?

_____

_____

_____

18. Vil en MLS-løsning sette større krav til brukerne enn dagens løsning?

- Ja
- Nei
- Vet ikke

Merknad: _____

_____

_____

Tusen takk for at du svarte!

Vedlegg D: Skjematiske resultater til kvalitativ undersøkelse 2

NB! Resultatene som er gjengitt under er gitt til denne oppgaven, og kan ikke brukes av andre uten samtykke!

1. Navn:

A	B	C	D

2. Stilling og arbeidssted:

A	B	C	D
?	?	?	?

3. Hvilke graderingsnivåer jobber du på?

A	B	C	D
Ugradert BEGRENSET HEMMELIG NATO SECRET	Ugradert BEGRENSET HEMMELIG NATO UNRESTRICTED NATO RESTRICTED NATO CONFIDENTIAL NATO SECRET	Ugradert BEGRENSET HEMMELIG NATO CONFIDENTIAL NATO SECRET	Ugradert BEGRENSET HEMMELIG NATO SECRET

4. Hvor lenge har du jobbet med de ulike nivåene?

A	B	C	D
2-3 år	0-1 år	2-3 år	2-3 år

5. Hvilke(t) nivå(er) jobber du på til daglig?

A	B	C	D
HEMMELIG NATO SECRET	NATO RESTRICTED NATO CONFIDENTIAL NATO SECRET	Ugradert BEGRENSET HEMMELIG NATO SECRET	Ugradert HEMMELIG NATO SECRET

6. Hvor ofte skifter du mellom å jobbe på de ulike nivåene?

A	B	C	D
Over 10 ganger dagelig	Over 10 ganger dagelig	4-10 ganger dagelig	4-10 ganger dagelig

7. Hvor mange forskjellige brukerstasjoner bruker du på en gjennomsnittlig arbeidsdag?

A	B	C	D
3	2	4 eller mer	3

8. Hvor ofte skifter du brukerstasjoner for å komme inn på forskjellige nivåer?

A	B	C	D
Over 10 ganger dagelig	1-3 ganger dagelig	4-10 ganger dagelig	1-3 ganger dagelig

9. Hvordan er brukervennligheten med dagens systemer/informasjonsflyt? (Svar gjerne med utfyllende kommentarer.)

Navn	Alternativ	Kommentar/Merknad
A	Lite god	Det medfører unødvendig mye ekstraarbeid at forskjellige graderinger ikke kan benyttes på forskjellige systemer. For å utføre primærfunksjon er det nødvendig å utveksle informasjon mellom systemer, og det tar uforholdsmessig mye ressurser å gjøre dette.
B	God	Ingen kommentar.
C	Lite god	Svært lite brukervennlig, da alt må tas ut på memostick som skal til et høyere graderingsnivå, og alts som skal til et lavere nivå må brennes ut på CD. Veldig tidkrevende.
D	Lite god	Ingen kommentar.

10. Føler du at dagens system er tungvindt på noen måte? Hvis Ja, utdyp i merknad.

Navn	Alternativ	Kommentar/Merknad
A	Ja	Et felles system for ulike graderingsnivåer hadde gjort informasjonsflyten enklere, for ikke å si mulig. Dette gjelder spesielt mellom norske og NATO-systemer.
B	Nei	Ingen kommentar.
C	Ja	Ingen kommentar.
D	Nei	Ingen kommentar.

11. Hvor mye av informasjon på de HEMMELIGE nettene kunne etter din mening, ha vært nedgradert?

Navn	Alternativ	Kommentar/Merknad
A	40 - 60 %	Jeg mener at bruken av nasjonale graderinger brukes i alt for stor grad. Det er innlysende at noe må holdes på nasjonalt nivå, men store deler av den informasjonen som i dag graderes nasjonalt kan etter min oppfatning gis en NATO-gradering. Dette vil gjøre forholdene bedre spesielt i multinasjonale miljøer.
B	40 - 60 %	Ingen kommentar
C	0 - 30 %	Ingen kommentar
D	0 - 30 %	Ingen kommentar

12. Finnes det mye lik informasjon på de ulike nettene?

Navn	Alternativ	Kommentar/Merknad
A	70 – 90 % er dupleks informasjon	Mitt svar her gjelder de nettene som ligger på H / NATO SECRET nivå.
B	10 – 30 % er dupleks informasjon	Ingen kommentar.
C	10 – 30 % er dupleks informasjon	Ingen kommentar.
D	10 – 30 % er dupleks informasjon	Ingen kommentar

13. Tror du at mye av informasjonen på det HEMMELIGE nettet, vil bli nedgradert til BEGRENSET, hvis Forsvaret innfører MLS?

Navn	Alternativ	Kommentar/Merknad
A	Ikke svart.	Vil ikke si at problemet er før høy gradering. Problemet er at ting gis en nasjonal gradering når en NATO-gradering like gjerne kunne vært gitt.
B	0-30 % av informasjonen vil bli nedgradert	Ingen kommentar.
C	0-30 % av informasjonen vil bli nedgradert	Ingen kommentar.
D	0-30 % av informasjonen vil bli nedgradert	Ingen kommentar.

14. Hvor lang tid tror du det vil ta før et MLS-system innføres i Forsvaret?

Navn	Alternativ	Kommentar/Merknad
A	Aldri	Dette er noe som krever evne, vilje og ikke minst penger. Jeg tror at evnen er der, til tider viljen – i hvert fall hos de som jobber i operative miljøer, men at det ikke kommer til å bli avsatt nok midler til å dekke inn økonomien. Noen vil kanskje se et slikt system innenfor sitt begrensede kontorlandskap, men de som har størst behov ikke vil se noe til systemet. Tviler sterkt på at det vil bli utplassert om lag 100 klienter i Kabul. Om systemet skal ha noen hensikt, er dette noe alle må ha tilgang til.
B	2-5 år	Ingen kommentar
C	6-10 år	Ingen kommentar
D	Aldri	Ingen kommentar

15. Vil MLS gjøre hverdagen enklere for deg? Hvis Ja, utdyp hvordan i merknad.

Navn	Alternativ	Kommentar/Merknad
A	Ja	Jeg vil med et slikt system kunne konsentrere meg om primærfunksjonen istedenfor å bruke ressurser på å skifte mellom ulike nett.
B	Vet ikke	Ingen kommentar
C	Ja	Det hadde jo vært greit å forholde seg til ett system, i stedet for 4. Spart mye tid på det, og ikke minst; ”hvor var det jeg hadde den filen igjen”?
D	Nei	Ingen kommentar.

16. Vil MLS forenkle informasjonsflyten? Hvis ja, utdyp i merknad.

Navn	Alternativ	Kommentar/Merknad
A	Ja	Jeg vil med et slikt system kunne konsentrere meg om primærfunksjonen istedenfor å bruke ressurser på å skifte mellom ulike nett.
B	Vet ikke	Ingen kommentar.
C	Ja	Ja, igjen ett system er raskere og enklere enn flere som man må veksle mellom.
D	Nei	Ingen kommentar.

17. Er det etter din mening noen spesielle prosesser som vil bli enklere ved en eventuell innføring av MLS?

Navn	Kommentar
A	Jeg vil med et slikt system kunne konsentrere meg om primærfunksjonen istedenfor å bruke ressurser på å skifte mellom ulike nett.
B	Ingen kommentar.
C	Ingen kommentar.
D	Ingen kommentar.

18. Vil en MLS-løsning sette større krav til brukerne enn dagens løsning?

Navn	Alternativ	Kommentar/Merknad
A	Ja	Vil kreve at hver enkelt bruker er bevisst på hvilken gradering som er gjeldene, for å hindre at uvedkommende får adgang til informasjon.
B	Vet ikke	
C	Nei	Antagelig lavere brukerterskel, men jeg vet ikke angående, miksing av de forskjellige graderte data. Tar maskinen hånd om det, eller er det bruker, gjennom brukerdefinisjon av etikett på dokumentet?
D	Ja	