Objektbaserad säkerhet

Behov och möjligheter

AMUND GUDMUNDSON HUNSTAD, TOMMY GUSTAFSSON,
HENRIK KARLZÉN, FREDRIK MÖRNESTEDT, LARS WESTERDAHL

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

Tel: 08-55 50 30 00
Fax: 08-55 50 31 00

www.foi.se

FOI-R--3484--SE
ISSN 1650-1942

September 2012

Amund Gudmundson Hunstad, Tommy Gustafsson, Henrik Karlzén, Fredrik Mörnestedt, Lars Westerdahl

Objektbaserad säkerhet

Behov och möjligheter

Titel	Objektbaserad säkerhet – Behov och möjligheter
Title	Object-Based Security – Needs and possibilities
Rapportnr/Report no	FOI-R--3484--SE
Månad/Month	September/September
Utgivningsår/Year	2012
Antal sidor/Pages	41 p
ISSN	1650-1942
Kund/Customer	Försvarsmakten
FoT område	Ledning och MSI
Projektnr/Project no	E36022
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informations- och aerosystem

Sammanfattning

Flexibilitet är en av de viktigaste egenskaperna hos en modern organisation. Medlemmar i organisationen arbetar både på och utanför arbetsplatsen, samarbeten mellan organisationer uppkommer plötsligt och kan avslutas snabbt. Det finns därför behov av hög tillgänglighet till information, med avseende på när, var och hur åtkomst sker.

En konsekvens av detta är att traditionella IT-säkerhetsmodeller med fokus på att skydda den skyddsvärda insidan mot den osäkra utsidan har svårt att stödja moderna organisationer på ett bra sätt. Detta hämmar verksamhetens mål och kan leda till genvägar där okontrollerade risker tas. I den här rapporten beskrivs förutsättningarna för objektbaserad säkerhet (OBS) som syftar till att skydda själva informationsobjektet istället för den infrastruktur det hanteras på. Detta förväntas ge hög tillgänglighet och flexibilitet men med bibehållen skyddsnivå.

Ett utsnitt av Försvarsmaktens informationsbehov samlades in genom en intervjuserie och påvisade stora variationer i behovet av information och hantering av densamma. Förutsättningarna för ett ledningssystem och ett kontorssystem i en utvecklingsverksamhet varierar betydligt. Vidare framgick att Försvarsmakten har behov av flexibla informationssystem med hög tillgänglighet.

Parallellt med intervjuerna genomfördes en litteraturstudie av aktiva forskningsinitiativ som kan göra det möjligt att realisera OBS. Resultaten från litteraturstudien och intervjuserien kombinerades sedan för att beskriva behov och möjligheter med OBS.

Nyckelord: Informationssäkerhet, Objektbaserad säkerhet, IT-säkerhetsmodell

Summary

Flexibility is one of the most important characteristics of a modern organization. Members of an organization conduct their work on-site as well as off-site, collaborations between organizations may start with little time for preparations and end just as quickly. This results in a need for high availability of information, both regarding access and available platforms.

As a consequence, traditional IT-security models with a focus on protecting the inside from the outside of a network have a difficult time supporting the needs of a modern organization. This inhibits the business goals of the organization and may lead to shortcuts with uncontrolled risks. This report describes the prerequisites for object-based security (OBS) which aims at protecting an information object, rather than the infrastructure that the information object resides on. This is expected to provide a high level of availability and flexibility while maintaining the proper level of protection.

An excerpt of the information needs of the Swedish Armed Forces was gathered through a series of interviews and showed large variations regarding the need for information and information management. The needs of a combat command and control system differ substantially from the needs of office systems. Furthermore, it was concluded that the Swedish Armed Forces need flexible information systems with a high degree of availability.

In parallel with the interviews, a literature study, regarding active research initiatives for realizing OBS, was conducted. The results from the literature study and the interviews were combined to describe the needs and possibilities of OBS.

Keywords: Information security, Object-based security, IT-security model

Innehållsförteckning

1 Inledning

Nyttjande av dagens informationstekniksystem (IT-system) kännetecknas av en hög grad av rörlighet. Konsumenterna är rörliga genom att de nyttjar sina verksamhetssystem dels på sin arbetsplats men även på resande fot samt hemifrån. De plattformar som används är bärbara och ibland mycket små, såsom mobiltelefoner. Även utanför arbetslivet utvecklas IT-system med fokus på hög tillgänglighet. Internetbaserade tjänster som webbaserad e-post och virtuella lagringsplatser är exempel på detta. Detta har resulterat i att konsumeten förväntar sig åtkomst till sina uppgifter eller sin arbetsgivares system, oberoende av var denne befinner sig. Program och uppgifter är mer sällan tillgängliga via fördefinierade datorer utan är tillgängliga via godtyckliga uppkopplade system Det gör att konsument sällan behöver befinna sig fysiskt nära det system som önskas åtkomst till.

Den verksamhet som en organisation bedriver är inte längre isolerad. Förutom medarbetares behov av åtkomst till organisationens system utanför arbetsplatsen så sker även samarbeten med andra organisationer som en normal del av verksamheten. Försvarsmakten har behov av att dela information med andra myndigheter, företag, internationella organisationer[1] samt icke-statliga organisationer[2]. Under vissa förutsättningar kan det även vara aktuellt att ge en annan organisation åtkomst till IT-system inom den egna domänen. Dessa samarbeten kan vara långsiktiga och planerade över en längre tid, men även mer hastigt påkomna under en pågående insats eller vid en katastrof.

Gemensamt för både en anställd och en privat konsument samt organisationer som skapar och förvaltar uppgifter är att uppgifter inte förväntas konsumeras på givna platser eller över givna system. Uppgifter och verksamhetssystem tillhandahålls över generella plattformar såsom webbläsare för att vara oberoende av mottagande system. Som en konsekvens håller en organisations fysiska gränser, det som utgör insida respektive utsida av organisationens IT-miljö, på att suddas ut. Den nya miljön ställer krav på att åtkomst till information är möjlig från flera platser. Samtidigt måste organisationen kunna kontrollera åtkomst till de uppgifter som anses skyddsvärda.

Ett IT-systems säkerhetsegenskaper beskrivs ofta med begreppen sekretess, riktighet och tillgänglighet från engelskans confidentiality, integrity och availability. Historiskt har sekretess varit den mest tongivande, vilket har resulterat i system som inte är anpassade för informationsutbyte med andra system eller som har mycket begränsande åtkomstkontroll. En verksamhet som

[1] Definition: En internationell organisation, exempelvis Nato, utgörs av stater.
[2] Definition: En icke-statlig organisation (eng. non-governmental organization, NGO) är en intresseorganisation där enskilda individer deltar av eget intresse. Exempel på en NGO är Läkare utan gränser.

kännetecknas av användare med hög mobilitet kräver en säkerhetsmodell som kan tillgodose alla säkerhetsegenskaper.

1.1 Mål och syfte

Det finns flera modeller som på olika sätt och med olika mognadsgrad kan hantera en verksamhetsmiljö med krav på flexibilitet och tillgänglighet. Exempel på sådana modeller är webbtjänster och Multi-Level Security. I denna rapport utreds förutsättningarna för en modell med objektbaserad säkerhet (OBS). Målet med rapporten är att definiera OBS och inom vilka gränser modellen är tillämpbar samt hur den matchar Försvarsmaktens informationssäkerhetsbehov.

Syftet med rapporten är att undersöka om OBS kan lösa Försvarsmaktens informationssäkerhetsbehov.

1.2 Avgränsning

För friare resonemang har ingen hänsyn tagits till existerande system inom Försvarsmakten eller hur i rapporten föreslagna initiativ förhåller sig till svensk lagstiftning samt Försvarsmaktens regler och interna bestämmelser.

1.3 Metod

En säkerhetsmodell kan endast vara meningsfull och effektiv om den stödjer det sätt som verksamheten i övrigt är utformad på. Om verksamheten har krav på tillgänglighet måste modellen kunna leverera uppgifter med hög grad av tillgänglighet samtidigt som behov av sekretess och riktighet tillgodoses. På samma sätt måste ett åtkomstkontrollerat system ha en säkerhetsmodell som prioriterar åtkomstkontroll. Av denna anledning genomfördes en intervjustudie i syfte att identifiera hur information och IT-system nyttjas inom olika delar av Försvarsmakten.

OBS är en relativt ny term och det finns flera andra namn på tekniker och modeller som har samma eller liknande syfte. Mångfalden av begrepp, i kombination med att området inte ännu är särskilt utforskat, har resulterat i en mängd olika uppfattningar om vad OBS är och på vilket sätt det kan bidra till att ge ett bra skydd för en organisations IT-system. För att identifiera vad som utgör kärnan inom OBS genomfördes en litteraturstudie där angränsande ansatser undersöktes.

1.3.1 Intervjuserie

Sex intervjuer genomfördes under maj 2012 med ett begränsat urval respondenter inom Försvarsmakten och FMV. Respondenterna representerade:

- Produkt- och systemägare med samordningsansvar för Försvarsmaktens IT-system
- Beställningsansvariga som omformar utvecklingsbehov till en konkret beställning
- Upphandlingsansvariga
- Operativt underrättelsearbete
- Operativt militärt arbete avseende utlandstjänst eller försvar av landet

Syftet med respondenternas skiftande vyer av det studerade problemområdet var att säkerställa en bredd i de inhämtade synpunkterna.

Intervjuerna genomfördes som kvalitativa intervjuer med fokus på ett avgränsat problemområde där respondenternas egna erfarenheter spelar en tydlig roll för förståelsen av problemområdet med en skriftlig intervjuguide som stöd (se bilaga A för intervjuguiden). Intervjuerna avsåg inhämta ett urval erfarenheter och synpunkter avseende dagens och framtidens informationssäkerhetsbehov inom Försvarsmakten. Speciellt fokus lades på situationer där beroenden av informationsinfrastrukturer är föränderliga och där informationsobjekten själva intar en tydlig roll avseende informationssäkerhetshantering. För att inte styra in respondenten på givna svar innehöll inte intervjuguiden några frågor om OBS. Däremot presenterades vid uppstarten av respektive intervju det projektsammanhang i vilket intervjuerna ingår. Avsikten är att identifierade verksamhetsbehov skall peka fram emot tänkbara lösningar. Med andra ord bör behovet av OBS baseras på en behovsanalys.

De flesta av intervjuerna spelades in, parallellt med att intervjuanteckningar gjordes. Inspelningarna gjordes för att komplettera anteckningarna vid behov. Inga fullständiga eller detaljerade transkriptioner av intervjuerna genomfördes. Intervjuanteckningarna lyfter därmed fram de, för det studerade problemområdet, viktigare huvuddragen i intervjuerna, men inte alla detaljer. En redovisning av intervjuanteckningarna redovisas i avsnitt 2.2.

Analys av intervjumaterialet genomfördes i form av läsning av intervjuanteckningarna och identifierande av informationssäkerhetsbehov respektive relevanta resonemang kring dessa.

1.3.2 Litteraturstudie

Litteraturstudien inleddes med att definiera begrepp och sökord med relevans för området utifrån tidigare forskning av FOI. Baserat på dessa sökord gjordes en första efterforskning med söktjänsterna Google Scholar, Scopus och Google. Därefter vidtog en genomläsning av den tidigare forskning vilken, baserat på artiklarnas sammanfattning, bedömdes ha relevans för OBS. Detta ledde fram till en diskussion om andra sökbegrepp som kunde vara av intresse vilka därefter eftersöktes på ovan nämnda söktjänster. Även de referenser som bedömdes intressanta i respektive artikel följdes upp. Stegen från sökning till uppföljning av referenser upprepades.

Olika kombinationer av följande sökbegrepp användes:

Initiala söktermer:	abac, användningskontroll, attribute based access control, cbis, ccn, content based information security, content centric networking, data centric security, distribuerad mac, dmac, infonet, mac, mandatory access control, mls, multi level security, netinf, network of information, object based security, object centric information security, object level protection, objektbaserad säkerhet, ucon, usage control
Härledda sökord:	abe, attribute based encryption, cac, cbi, ccnx, cryptographic access control, ibe, identity based encryption, mic, nato, uconabc

1.4 Rapportstruktur

Rapporten presenterar inledningsvis (kapitel 2) en sammanfattning av de intervjuer som genomförts. Därefter, i kapitel 3, beskrivs de initiativ som är aktiva inom eller i anslutning till problemområdet. De båda inledande kapitlen analyseras i kapitel 4 och resultatet diskuteras i kapitel 5. Avslutningsvis preciseras slutsatser och idéer om fortsatt arbete i kapitel 6.

2 Intervjuserie: informations-säkerhet inom Försvarsmakten

Vid val och uppbyggande av säkerhetslösning är det av vikt att säkerställa att lösningen stödjer den verksamhet som bedrivs. Detta implicerar vikten av att inventera vilka informationssäkerhetsbehov som existerar inom Försvarsmakten. Som utgångspunkt för behovsinventeringen redovisas i detta kapitel:

- Försvarsmaktens strategiska avvägningar och målbild med inverkan på informationssäkerhet inom Försvarsmakten
- Huvuddragen i vad som yttrades vid intervjuerna under maj 2012 avseende informationssäkerhetsbehov inom Försvarsmakten

2.1 Bakgrund

En utgångspunkt för Försvarsmaktsarbete avseende informationshantering och för detta nödvändig informationsinfrastruktur, utgörs av CIO:s formulerade vision i CIO:s strategidokument (Försvarsmakten, 2008):

Försvarsmakten skall ha en tillgänglig, säker och kostnadseffektiv informationshantering och informationsinfrastruktur- ” här och nu” samt över tiden för hela verksamhetens behov där vår insatsförmåga sätts i fokus.

CIO:s vision utmynnar i strategidokumentet i en diskussion med utgångspunkt i ett antal målområden av vikt för utvecklingen inom informationshanterings- och informationsinfrastrukturområdet. Dessa målområden är relaterade till personalfrågor, interoperabilitet, nyttjande av datornätverk och modern teknik, effektiv ledning och styrning av IT-verksamhet, god IT-ekonomi, effektiv myndighetsutövning, effektiva informationsresurser och väl utvecklad informationssäkerhet. De olika målområdena ses som delar av en helhet utan inbördes prioritering.

För att realisera CIO:s vision, och med utgångspunkt i de formulerade och diskuterade målområdena, presenterar måldokumentet (Försvarsmakten, 2009) vikten av att ta fram en nät- och informationsinfrastruktur (NII) för Försvarsmakten. NII definieras som *den infrastruktur som erfordras för att olika grupperingar av användare inom Försvarsmakten skall kunna få tillgång till och ge tillgång till informationstjänster lokalt, nationellt och internationellt i olika koalitioner och i federationer av system*.

Måldokumentet formulerar en principplan och styrning för specificering av förmågekrav på NII. Vikten av effektiv, säker och rationell

informationshantering inom Försvarsmakten lyfts fram. För detta är det nödvändigt att inventera vilka resurser och strukturer som krävs för att realisera visionen. Fokus i denna inventering är på vilka tjänster rörande kommunikation respektive informations- och integrationstjänster som behövs samt förvaltning och drift av NII. För detta identifieras ekonomiska, organisatoriska, juridiska samt säkerhetsrelaterade konsekvenser och beslutspunkter samt mål formuleras.

Måldokumentet påpekar vidare att arbetet med informationssäkerhet behöver sättas i Försvarsmaktssammanhang och fokusera på skydd av för Försvarsmaktens vitala värden. Informationssäkerhetens roll som möjliggörare, och att därmed förbättra förmågan att dra nytta av utvecklingen på IT-området, accentueras.

NATO Network Enabled Capabilities (NNEC) Technical Services Model skall enligt (Försvarsmakten, 2009) användas för att åstadkomma tänkt nät- och informationsinfrastruktur (NII) för Försvarsmakten. I detta arbete är en bärande idé att *en och endast en gemensam nät- och informationsinfrastruktur [..] på ett ensat sätt ska skapa interoperabilitet och flexibilitet för både fred och insats.* Information och tjänster skall därigenom vara tillgängliga och en föränderlig miljö skall enkelt kunna hanteras. NNEC lyfts fram av måldokumentet som ett ramverk för att beskriva CIO:s *mål inom de olika delarna av NII samt att avgränsa NII från den kravställande verksamheten*. Harmonisering med relaterade NATO-satsningar underlättas också.

Denna målsättning innebär betydande utmaningar. Dagens infrastruktur bygger på säkerhetsdomäner med särskilda godkända separationsmekanismer, med associerade betydande kostnader for att underhålla separata infrastrukturmiljöer. Detta innebär tillgänglighetsbegräsningar och risk för att information manuellt överförs mellan olika domäner och förbi separationsmekanismerna. Vad NII siktar på är att koppla samman olika säkerhetsdomäner och verksamhetszoner, och samtidigt på ett godkänt sätt kunna erbjuda tjänster över hela infrastrukturen, med adekvat informationssäkerhet, önskvärt informationsutbyte och flexibilitet. NII innebär kommunikationsmässigt inte att alla infrastrukturdelar alltid behöver vara fysiskt sammankopplade. Däremot skall det vid behov och beslut vara möjligt att sammanfoga delarna utan omfattande omkonstruktion. I detta sammanhang blir idéer som OBS, där informationsobjekt skyddas i sig själva, intressanta att beakta.

2.2 Variationsrikedom bland Försvarsmaktens verksamhet

Försvarsmakten är en stor organisation med många typer av verksamhet och i detta avsnitt redovisas de olika respondenternas intryck om detta.

2.2.1 Militära typsituationer

En utgångspunkt för respondenternas resonemang under intervjuerna var en mycket förenklad struktur, enligt Bilaga B, över för Försvarsmaktsaktörer olika relevanta typsituationer som patrullering, krigsliknande situation och fredsliknande situation. Typsituationerna anges som funktioner av ledningsnivå (från grupp- till brigadnivå).

Skillnaderna mellan krig och strid i Bilaga B upplevdes av respondenterna som mindre tydliga och en respondent ansåg att ungefär samma informationsbehov uppstår i freds- och patrullsituationer som i krig och strid.

Flera av respondenterna anmärkte på att tabellen över militära typsituationer saknade fredssituationens produktion och rent myndighetsarbete med fokus på administrativt kontorsarbete. Denna typsituation ansågs vara helt olik insatsorganisationen.

2.2.2 Ledningsnivådimensionen

En av dimensionerna av tabellen i Bilaga B är de olika ledningsnivåerna från grupp- till brigadnivå. Respondenterna såg väsentliga skillnader mellan dessa. En respondent ansåg att detta medför att gemensamma stabsstöd och lägesbilder på alla nivåer inte är någon god idé och att fokus istället borde vara på att ge varje användare rätt utsnitt. En annan vanlig observation från intervjuerna var att behov av hög mobilitet präglar lägre ledningsnivåer till skillnad från de högre.

Visionen i (Försvarsmakten, 2009) om en och endast en informationsinfrastruktur tolkade en respondent som att uppdelade kommunikationsnät avses, men att kryptoprodukter är likartade även om de kan variera något inom infrastrukturen. Varierande behov innebär att olika tekniska lösningar är lämpliga, exempelvis med avseende på snabbhet i fält eller den större mängden information som hanteras i kontorsmiljö. Intervjupersonen trodde därför inte på någon större homogenisering av system utan istället främst bibehållen diversifiering per verksamhetstyp. En annan respondent menade att just skillnaden i tidskritiskhet, tillsammans med varierande typer av information, gör *ett och endast ett nät* mindre intressant över ledningsnivåerna, särskilt då under bataljonsnivå.

Flera respondenter lyfte fram att operativ verksamhet ibland måste bryta mot fastställda regler för att prioritera att rädda liv, varför verkan går före skydd eller rent av är en form av skydd. Det kan innebära att man tvingas att ta sig runt säkerhetsskydd med hjälp av *klister och tejp*, såsom att flytta data med hjälp av CD-skivor mellan system i olika säkerhetszoner eller genom att skruva upp och koppla förbi kryptomaskiner. En annan möjlighet är att exempelvis tvingas avslöja sin position för en fiende för att undvika vådaskjutning. Det är därför enklare att följa reglerna på planeringsnivå än på operativ nivå. Samtidigt är det

viktigare att skydda affärshemligheter på högre nivå. En respondent bedömde det som ovanligt att mer insatsnära befäl direkt berörs av sekretessfrågor, bland annat eftersom det är ovanligt att officerare på lägre nivå måste hemlighålla information från sina underordnade.

En annan respondent tyckte vidare att ytterligare en ledningsnivå, ovanför de andra, behövs i Bilaga B för att återspegla Försvarsmaktens organisation och verksamhet. Denna strategiska nivå medför en annan och annorlunda informationsmängd, samt tillgång till ett större stabsstöd.

2.2.3 Tidsdimensionen

Bilaga B saknar enligt flera respondenter tid som dimension. Operativ verksamhet är ofta känslig bara fram tills att operationen har genomförts, medan strategisk information är mer långsiktig och därför också har behov av mer långsiktigt skydd. Dessutom avslöjas information genom operativt agerande vilket gör att en del information inte längre kan ses som känslig då den får bedömas vara röjd. En annan aspekt är att till exempel kryptografiska lösningar kan vara alltför långsamma eller omständliga för tidskritiska fältapplikationer.

En respondent lyfte fram att på lägre mer stridsnära nivåer finns behov av att fatta snabbare beslut vilket medför behov av begränsade informationsmängder och, åtminstone till viss del, färdiganalyserat beslutsunderlag samt automatiserade metoder för exempelvis riskvärdering. I en annan intervju noterades att informationsmängderna växer och växer med utvecklingen vilket kan ställa till med ytterligare problem. Exempelvis kan det bli svårt att i realtid sammanställa all sensorinformation. En omfattande volym sensorinformation kan därigenom innebära en överbelastning, vilken i nästa steg kan medföra att skyddsförmågan minskar. På högre nivå finns däremot bättre möjligheter att hantera stora mängder information eftersom stabsfunktionen är större och verksamheten sällan lika tidskritisk.

Längre insatser medför andra behov än kortare insatser. I rena krigssituationer rör det sig oftast om kortare insatser på högst några månader medan fredsbevarande insatser kan pågå i åratal. I det senare fallet kommer därmed flera generationer soldater att arbeta med informationen och därmed ärva den från varandra, vilket innebär särskilda behov vad gäller informationens riktighet, lättförståelighet, att den är uppdaterad samt att den överhuvudtaget går att finna. I och med införandet av ett yrkesförsvar, som på ett annat sätt skiljer krigsförbanden från administrationen, accentueras dessa aspekter.

2.2.4 Interaktionsdimensionen

Samarbete med civila aktörer är ytterligare en viktig aspekt som respondenterna saknade i Bilaga B. Bland civila aktörer kan det vid exempelvis utlandsuppdrag

förekomma betydande begränsningar i vilka tekniska och säkerhetsmässiga resurser som finns. Tillgängliga resurser kan vara otillräckliga och omoderna. Ibland krävs dessutom samarbete med aktörer man inte planerat eller förutsett samarbete med, eller som normalt inte ses som allierade. I sådana situationer föreligger stort behov av att korrekt information delas för att undvika situationer där det framstår som att man försöker lura sina allierade.

Koalitioner ger också komplexa säkerhetspolicyer eftersom medlemmarnas interna regelverk varierar. Ett intressant problem rörande tillgänglighet och sekretess uppstår när Försvarsmakten hämtar NATO-uppgifter från en källa på internet, bara för att ofta tvingas klassificera informationen som belagd med utrikessekretess. Sådan information kan då inte hanteras på en internetansluten dator vilket innebär att informationen måste flyttas från det system som inhämtade informationen.

En respondent tryckte även på en annan aspekt, nämligen interaktion med motståndare. Det skydd som behövs varierar med motståndaren – huruvida det till exempel rör sig om en likvärdig motståndare eller en motståndare som utövar assymmetrisk krigföring.

2.3 Informationssäkerhetsegenskaper

Vid intervjuerna framkom att ett antal olika informationssäkerhetsegenskaper påverkar behoven.

2.3.1 Sekretess och tillgänglighet

Flera respondenter indikerade att det ofta är svårt att göra avvägningen mellan tillgänglighet och sekretess. På många ställen i Försvarsmakten är idag sekretessnivån gränssättande men i stridssituationer ökar behovet avseende tillgänglighet till information och, som nämndes vid redovisningen av skillnader mellan ledningsnivåer, går verkan ibland före skydd. En respondent utvecklade det hela och nämnde att informationsbrist sällan är ett problem i fält och att ämnesrelevant information dessutom normalt finns att tillgå. Däremot kan informationen i vissa fall vara för gammal och i behov av uppdatering. Ett problem är dock samtidigt att det kan vara svårt att veta att en viss typ av information ens existerar. Det är därför viktigt att det redan vid inhämtning eller skapande av information identifieras vilka roller och individer som kan vara i behov av informationen.

Ett problem för tillgängligheten är att information hålls otillgänglig en period och sekretessen prioriteras därmed. Ett sådant förfarande kan bero på att det bedömts att arbetsdokument inte bör spridas, då de kan vara otillräckliga eller vilseledande för läsaren eftersom slutversionen kan komma att se annorlunda ut. Användarvänlighet, och därmed tillgänglighet, blir dock en allt viktigare aspekt

för IT-system, enligt respondenterna. Alltför komplexa säkerhetslösningar kommer trots allt att antingen användas fel, eller inte alls.

En stor utmaning rörande sekretess och tillgänglighet, som togs upp i intervjuerna, är ekonomisystemet Prio, som handhar H/R-uppgifter och måste kunna kommunicera med externa myndigheters, eventuellt öppna, system. Detta medför stora behov av säkerhetsmekanismer som balanserar sekretess- och tillgänglighetskrav. Personlig integritet är också av vikt att beakta, bland annat rörande lönesamtal, sjukdom och övrig känslig information.

Det är, enligt respondenterna, av vikt att kravställare förstår verksamheten i övrigt, så att säkerhetsstöd utformas utifrån de behov som finns. Dessutom behöver den ekonomiska aspekten kring säkerhet och faktiska nyttokalkyler belysas ytterligare, enligt en intervjuperson. Nyttan med allt som görs måste dessutom bli tydligare. Därmed kan man undvika att utstätta sig för säkerhetsrisker, genom att först säkerställa att positiva effekter uppnås med valda åtgärder. Ett exempel är sociala medier där nyttovärdering är viktig, men även utbildning och attitydsförändring är av vikt. Sociala medier kan utgöra en stor fara när information läcker ut, hanteras fel eller misstolkas.

Vidare läggs i dagsläget mycket skydd på en liten, men särskilt skyddsvärd, del av informationen, medan små resurser läggs på att skydda den övriga, stora mängden mindre skyddsvärd information. Då tas det inte med i beräkningen att stora informationsmängder bildar aggregat som tillsammans kan bli mer skyddsvärda än deras beståndsdelar. Här bör det även beaktas att det ofta används osäkra kanaler vid överföring av information som inte i egentlig mening är hemlig, men som ändå inte bör spridas fritt.

En annan aspekt på området sekretess kontra tillgänglighet, som nämndes av en respondent, rör signalskydd. Signalskydd har bland annat som ändamål att avlyssningsskydda trafik för att undvika att motståndaren kan nyttja trafikinformation för att skapa störningar i nätet. Därmed kan en form av sekretesskydd samtidigt ge ökad tillgänglighet.

En respondent påpekade att där sekretessnivån idag är gränssättande, kommer framtida behov i större grad röra andra säkerhetsaspekter. Exempelvis kommer aktuell hotbild respektive operations- och insatsmiljöns begränsningar och möjligheter att vägas in mer aktivt.

2.3.2 Riktighet

Intervjuerna visade att riktighet är en säkerhetsegenskap som inte har fått så mycket fokus i säkerhetsarbetet inom Försvarsmakten. Tillgång till korrekt information blir mer kritiskt i strid, särskilt eftersom man har kort tid på sig att åtgärda eventuella brister i informationen. Dessutom är riktighet viktigt i samband med autentisering. Att med autentisering avgöra om system och

användare är vilka de säger sig vara är inte bara intressant för att besluta om tillgång till information utan också för att se till att inte legitima system och användare kommunicerar med illegitima sådana. Vidare är spårbarhet viktig för att kunna utkräva ansvar och se till att reglerna inte är uddlösa. Samtidigt måste spårbarhet vägas mot övervakning och intrång i den personliga integriteten. Tekniskt skydd av riktighet är viktigt men kritisk granskning av information, såsom sensorinformation, är ett komplement, menade en respondent.

2.3.3 Påverkan av centralisering eller distribuering

Flera respondenter satte fokus på att i fred så är personal i mindre utsträckning distribuerad, vilket innebär att centraliserad datadrift passar bättre. Vidare nämndes att det är naturligt att IT-lösningar börjar som ad hoc på enskilda förband för att därefter sammanföras centralt. I strid finns å andra sidan behov av distribuering. Nuförtiden har även mindre patrullerande grupperingar ofta med sig kontorssystem vilket behövs för exempelvis tidrapportering. Kanske kan privata, det vill säga Försvarsmakts- eller myndighetsinterna, moln vara intressanta för en avvägning mellan distribuering och centralisering.

Under kalla kriget var det svenska försvarets enheter designade att agera autonomt och irreguljärt – *som arga bin* uttryckte sig en respondent – och därmed distribuerat. Nu är ett sådant förfarande oförsvarbart ur ekonomisk synvinkel varför mer och mer centraliseras. Å andra sidan kan situationer där autonomt och mobilt agerande behövs komma att bli vanligare. För att upprätthålla autonomitet är distribuering viktig, vilket försvåras av centraliserad informationshantering. Hårddisklösa tunna klienter togs dock upp av en respondent som intressanta för att ge ökad säkerhet eftersom lokal information raderas vid avstängning. Det bristande perimeterskyddet är därmed ett mindre problem även om en sådan lösning leder till mer begränsad tillgänglighet.

I flera intervjuer framkom att det nuförtiden är vanligare att individer arbetar hemifrån, har andra arbetstider eller använder egna enheter såsom smarta telefoner, ibland benämnt bring-your-own-device (BYOD). Detta ger ett mer distribuerat arbetssätt samt en blandning av privat och arbetsrelaterad teknisk utrustning. Användande av privat utrustning ger nya säkerhetsrelaterade utmaningar som uppstår på grund av bristande kontroll. Lathet såväl som ekonomiska faktorer kan förstärka BYOD-trenden och även om de tekniska aspekterna av trenden finns delvist belysta är det enligt en respondent mer oklart hur regelverk och policyer ska utformas. Välfärdssystem[3] som sociala medier är visserligen inte tunga applikationer och kan använda egna

[3] Välfärdssystem är en benämning på IT-system som är till för individens personliga välmående. Det kan till exempel omfatta datorer där soldaten kan hålla kontakt med anhöriga via e-post och sociala medier.

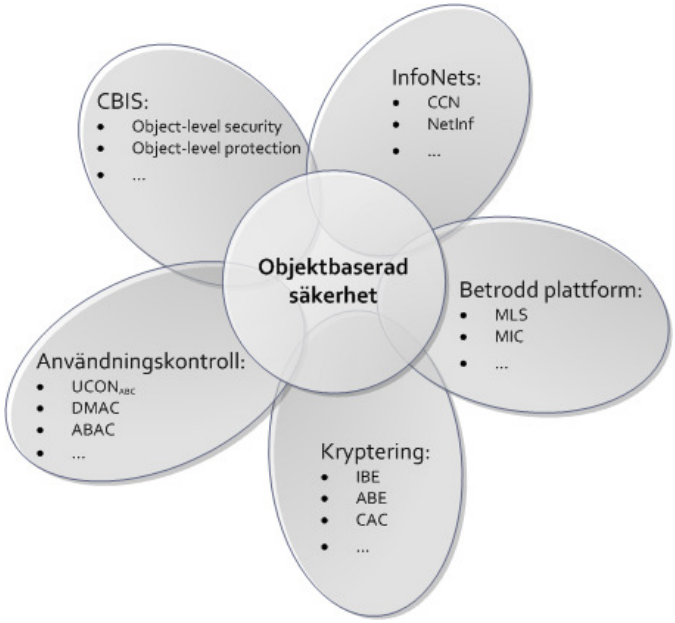
kommunikationskanaler, men i längre utlandstjänst kan de ändå leda till begränsningar i näten, genom att de används mer än vid kortare uppdrag.

Flera respondenter lyfte fram spårbarhet och en annan typ av infrastruktur, som inte baserar sig på perimeterskydd, som medel för att minska problemen som uppstår på grund av distribueringen. När informationsinfrastrukturen är oberoende av applikationerna behövs en infrastruktur per sekretessklass och det kan vara lämpligare med enbart enklare skyddsmekanismer i infrastrukturen och mer komplexa sådana i objekten, i likhet med tankegångarna i FMLS 2010. Det tar dock lång tid att ändra synsätt även om en del tester med det närbesläktade ämnet attributbaserad säkerhet genomförts. Slutligen är även insiderproblematiken fortfarande en utmaning, vilket flera respondenter tryckte på.

3 Litteraturstudie

För att kartlägga de mekanismer som skulle kunna användas för att implementera OBS genomfördes en litteraturstudie över närliggande forskning. Där så var möjligt grupperades forskningen in under generaliserade termer såsom användningskontroll och kryptering.

Figur 1 visar de forskningsområden som bedöms mest relevanta för OBS samt exempel på inriktningar inom dessa områden.



Figur 1: Forskningsområden relaterade till OBS.

OBS-system kommer att byggas upp av flera olika säkerhetsmekanismer såsom användningskontroll och kryptering. Det är ett system som helt eller delvis delar teknik med ett eller flera andra forskningsområden. Det är också tänkbart att det finns mekanismer som ännu inte är helt utvecklade.

3.1 Användningskontroll

Användningskontroll är en direktöversättning av engelskans Usage Control (UCON) och är ett begrepp som Park och Sandhu (2004) beskriver som en generalisering av åtkomstkontroll[4]. Traditionell åtkomstkontroll hanterar enligt

[4] Eng. access control

samma källa endast autentisering och auktorisation i samband med att ett dokument öppnas och kan därför inte hantera kontinuerlig användningskontroll.

Området kan i princip indelas i två fokus, kontinuerlig autentisering och kontinuerlig auktorisation. Kontinuerlig autentisering handlar precis som traditionell autentisering om att avgöra vem som är behörig till ett objekt, men sker löpande under tiden som objektet är öppet till skillnad för att endast ske vid själva öppnandet. Kontinuerlig auktorisation fokuserar på vad vederbörande får göra med objektet, till exempel om denne får skriva ut eller kopiera objektet, under hela åtkomsten. Detta kan även omfatta regler för hur ett IT-system får hantera objektet, till exempel vilka nätverksnoder det får passera och vilka enheter det får lagras på.

Användningskontroll är ett omfattande forskningsområde och därför begränsas litteraturstudien till modellen $UCON_{abc}$[5] eftersom den täcker in flera andra modeller samt distributed mandatory access control (DMAC) eftersom den innehåller ett distribuerat tankesätt. I kombination med tidigare forskning inom attributbaserad åtkomstkontroll i projektet Objekt och tjänstebaserad säkerhet (Westerdahl, 2011) bedömdes detta ge en tillfredställande översikt av området användningskontroll.

3.1.1 $UCON_{abc}$

$UCON_{abc}$ är en metod för användningskontroll för vilken Park och Sandhu (2004) definierat en familj med modeller som beskriver hur ett informationsobjekt får användas. Dessa modeller är en generalisering av åtkomstkontroll och omfattar autentisering och auktorisation samt kontroll av förpliktelser, villkor och riktighet. Förpliktelser avser attribut som kopplas till subjektet eller objektet och som måste vara uppfyllda, till exempel att ett licensavtal undertecknas innan öppnandet. Villkor avser attribut som är oberoende av subjektet och objektet såsom miljö- eller systemkrav och kan till exempel vara att subjektet finns på en viss geografisk position.

Kontrollerna sker både vid öppnande av ett objekt och kontinuerligt under dess användning. Metoden tillåter också att användarens aktiviteter kan förändra subjektens och objektens attribut före, under eller efter användningen av ett objekt.

Modellerna utgör ett beskrivningsspråk för policyer och kan även användas för att beskriva andra mekanismer för användningskontroll och åtkomstkontroll såsom mandatory access control (MAC), discretionary access control (DAC),

[5] Indexet ABC står för de beslutsfaktorer som används för att styra användningen av ett objekt nämligen auktorisation (Authorization), förpliktelser (oBligations) och villkor (Conditions).

digital rights management (DRM), role-based access control (RBAC) och trust management (TM) (Lazouski, Martinelli och Mori, 2010).

$UCON_{abc}$ är endast en teoretisk metod men det finns ett par artiklar som beskriver hur ett konkret införande av modellerna skulle kunna ske med dagens teknik. Zhang, Nakae, Covington och Sandhu (2008) beskriver modellernas tillämpning på ett så kallat samverkande IT-system, där användare delar med sig av sina datorresurser, men denna beskrivning hanterar inte distribuerade system. Stihler, Olivo Santin, Calsavara och Marcon Jr. (2009) beskriver däremot en arkitektur som kan användas för distribuerad användningskontroll.

3.1.2 Distribuerad MAC – DMAC

Begreppet mandatory access control (MAC) refererar till en typ av åtkomstkontroll där operativsystemet begränsar ett subjekts tillgång till ett objekt. Ett objekt kan till exempel vara en fil, dataström eller en dataport. Subjektet behöver inte vara en fysisk användare utan kan även vara en process eller en tjänst.

Både subjekt och objekt har attribut kopplade till sig. Attributen testas mot en policy när ett subjekt begär tillgång till ett objekt. En policy i DMAC är ett regelverk uppsatt för att styra vad ett subjekt får göra med ett objekt. Policyn kan inte påverkas av användaren utan styrs centralt av en administratör.

Distribuerad MAC (DMAC) skiljer sig mot MAC på så vis att åtkomstkontrollen kan utökas till datorer som inte nödvändigtvis befinner sig inom samma säkerhetsdomän som informationsägaren. Detta kan uppnås genom att de system som utför åtkomstkontrollen i respektive säkerhetsdomän utbyter information med varandra. DMAC används som en lösning i till exempel beräkningskluster och molntjänster, ofta då i samband med virtuella maskiner (Zou, 2009).

3.2 Kryptografi

Kryptografi är ett område med omfattande forskning och där olika krypteringsmetoder kan användas för att bygga upp OBS. Kryptering kan i huvudsak användas för att upprätthålla ett objekts sekretess och integritet när det är i rörelse eller vila och bara till begränsad omfattning när objektet är under användning.

Nedan presenteras ett par krypteringsområden som bedöms vara av särskilt intresse för OBS.

3.2.1 Identitetsbaserad kryptering

Identitetsbaserad kryptering (Identity-based encryption, IBE) analyserades av Shamir (1984) och är i grunden en assymmetrisk krypteringsmetod som använder

en publik och en privat nyckel men utan att avsändaren av ett krypterat meddelande först måste hämta mottagarens publika nyckel. Istället fungerar en allmänt tillgänglig uppgift, till exempel en e-postadress eller ett användarnamn, som publik nyckel. Den tillhörande privata nyckeln kan mottagaren generera hos en viss pålitlig tredje part.

3.2.2 Attributbaserad kryptering

Attributbaserad kryptering (Attribute Based Encryption, ABE) är en krypteringsapplikation som baseras på en krypteringsmetod som kallas Fuzzy Identity-Based Encryption (FIBE) (Sahai och Waters, 2004). FIBE är en vidareutveckling av IBE och tillåter en viss diskrepans mellan den nyckel som skapar en kryptotext och den nyckel som används för att dekryptera den.

Denna diskrepans kan utnyttjas för att skapa en krypteringsnyckel som består av flera attribut som kan kopplas till en användare, till exempel avdelning, position och system. Alla användare som uppfyller dessa attribut kommer då att ha möjlighet att få tag i den privata nyckeln från en viss tredje part och därmed dekryptera meddelandet.

I sin ursprungliga beskrivning av ABE nämner Sahai och Waters (2004) att ett intressant problem som återstår att lösa är huruvida de attribut som genererar nycklar kan komma från flera parter. Müller, Katzenbeisser och Eckert (2009) presenterar en teknik som de kallar distribuerad ABE och som skulle göra det möjligt att låta flera parter hantera attribut och tillhörande privata nycklar.

3.2.3 Kryptografisk åtkomstkontroll

Kryptografisk åtkomstkontroll (Cryptographic Access Control, CAC) syftar till att ersätta så kallade referensmonitorer[6] med kryptering för att åstadkomma en typ av åtkomstkontroll (Harrington och Jensen, 2003). Referensmonitorer kan jämföras med ett kontrollcenter som autentiserar subjekt och som implementerar och effektuerar gällande säkerhetspolicy för åtkomst till ett objekt. Referensmonitorer är systembundna och är därför svåra att använda som kontrollmekanismer inom OBS.

CAC löser problemet med referensmonitorernas systembindning genom att använda kryptering som kontrollmekanism. CAC innebär enkelt uttryckt att det endast är den som är behörig till ett objekt som kan dekryptera det eftersom endast denne får ta del av dekrypteringsnyckeln.

[6] Eng. reference monitors

I och med paradigmen med distribuerade datorsystem har CAC blivit en högintressant teknik eftersom den kan användas för att säkerställa sekretessen och riktigheten för objekt som hanteras utanför den egna IT-plattformen.

3.3 Betrodd plattform

För att isolera ett objekt under användning kan en betrodd plattform användas. Sådana plattformar är föremål för ett kommande forskningsprojekt inom FOI och vissa tekniker av särskilt intresse för OBS presenteras nedan.

3.3.1 Multi-Level Security – MLS

Multi-Level Security (MLS) avser säkerheten i ett system som reglerar hantering av information på olika sekretessnivåer i ett och samma system (SIS, 2007). Detta innebär att MLS fokuserar på att skydda objekt under användning men hanterar inte objekt under rörelse eller i vila. MLS är ett område där mycket forskning har förekommit och Kiviharju (u.å.) redogör för hur MLS kan användas tillsammans med CAC och ett XML-baserat filformat för att uppnå CBIS-liknande egenskaper (se även avsnitt 3.5).

3.3.2 Mandatory Integrity Control – MIC

Mandatory Integrity Control (MIC) är en säkerhetsteknik från Microsoft som introducerades i Windows Vista (Riley, 2006). Tekniken är inriktad på att isolera olika processer som körs i en inloggningssession från varandra. Teknikens mål är att separera olika programkomponenter beroende på kontext. Programkod som kommer från en potentiellt mindre tillförlitlig källa som till exempel webben får inte samma rättigheter som den kod som kommer från en mer tillförlitlig källa, som den lokala hårddisken.

3.4 Informationsfokuserade nätverk

Dagens datornätverk är värdfokuserade eftersom varje dator har en adress som används för att komma åt datorn och dess information. Jacobson, Mosko, Smetters och Garcia-Luna-Aceves (2007) förordar därför att nästa generations Internet skall utvecklas och att detta skall fokusera på information istället för på värdar. Denna generation har i denna rapport valts att kalla informationsfokuserade nätverk som är en fri översättning av information-centric networks eller network of information som är allmänt använda engelska namn.

Informationsfokuserade nätverk är ett område som drivs parallellt i flera forskningsinitiativ i världen. Två av de som har kommit långt inom området är EU-finansierade Network of Information och Content-Centric Networking. Dessa påminner i mångt och mycket om varandra men det finns skillnader i till exempel namngivningen av objekt.

3.4.1 Network of Information – NetInf

Grunden för Network of Information (NetInf) är ett informationsfokuserat nätverk (NetInf, 2012). Det viktiga är tillgången till efterfrågad information, inte var den är lagrad. För att få detta att fungera är all information förpackad som informationsobjekt (IO) där varje IO är unikt identifierbart.

NetInf har flera likheter med OBS, till dessa hör bland annat unik identitet för varje IO, signaturer för att märka IO med avsändarens identitet, skydd av attribut från obehörig ändring och kryptering av IO.

3.4.2 Content Centric Networking – CCN

Problemställningen inom Content Centric Networking (CCN) är densamma som för NetInf, att skapa nästa generations nätverksarkitektur. En av de drivande inom detta område är Palo Alto Research Center (CCN, 2012). Målsättningen är att skapa en enkel, universell och flexibel kommunikationsarkitektur som kan lösa dagens och morgondagens kommunikationsproblem. Arkitekturen skall vara minst lika skalbar och effektiv som TCP/IP och dessutom säkrare samt kräva mindre konfiguration.

För att kunna prova idéerna med CCN har det öppna källkodsprojektet CCNx skapats (CCNx, 2012). Projektet befinner sig i en tidig utvecklingsfas men redan nu finns ett antal projekt som drivs av olika organisationer där CCNx används som en grund vid bygget av egna experiment.

3.5 Content Based Information Security – CBIS

Content Based Information Security (CBIS) är ett begrepp som myntades av amerikanska försvarsmakten år 2000 (McGovern, 2001). Målsättningen var att åstadkomma säker informationshantering mellan olika säkerhetsdomäner. Det ursprungliga projektet avslutades 2005 och därefter har forskningsområdet CBIS splittrats upp i flera andra områden såsom object-level security och object-level protection. Sökning har skett på dessa termer men det har inte gått att få fram någon relevant information kring dessa.

Den finländska försvarsmakten har valt att fortsätta med beteckningen CBIS i flera projekt mellan 2005 och 2010. I dessa projekt har bland annat två demonstratorer byggts upp med målet att vara användbara verktyg (Kiviharju, 2010). Ett vägval som har gjorts är att inrikta sig på filformaten för Microsoft Powerpoint, Microsoft Word och ett mer generellt XML-liknande dokumentformat. Vidare fokuserar dessa demonstratorer inte enbart på objekten utan värderar även enskild information inom respektive objekt.

4 Analys

I detta kapitel sammanställs analysen av de intervjuer som genomfördes med personal från Försvarsmakten och FMV. Dessutom presenteras de förmågor som OBS bör ha, vilka funktioner som levererar dessa förmågor samt hur den relaterade forskningen förhåller sig till OBS.

4.1 Intervjuanalys: behovsbild

Intervjumaterialet redovisar, trots att antalet respondenter var begränsat, en bredd av synsätt och uppfattningar om Försvarsmaktens verksamhet samt informationssäkerhetsbehov som verksamheten ger upphov till. Detta talar för intervjumaterialets relevans som underlag för en bild av informationssäkerhetsbehoven inom Försvarsmakten.

Behov som framkom vid intervjuerna är beskrivna på en övergripande nivå, vilket sannolikt är ett resultat av att ställda frågor var övergripande. Dessa behov kräver djupare studier med mer indata för att kunna resultera i mer detaljerade behov.

Ett begränsat antal tongivande spår återkom i de olika intervjuerna, varför behovsresonemangen har grupperats efter dessa.

4.1.1 Verksamhetsfokus

Försvarsmaktens resurser används på ett flertal olika sätt av användarna, såväl på grund av olika uppgifter som skall lösas, som önskemål att utnyttja nya tekniska möjligheter. Företeelser som BYOD-trenden påverkar därmed även Försvarsmakten med nya förväntningar och behov.

Det är av vikt att klargöra skillnader mellan verksamhetsplanering och operativ verksamhet, och låta dessa påverka behovsinventeringen. Skillnaderna pekar på viktiga avvägningar rörande till exempel lägesbildshantering och visionen om ett och endast ett nät. Vad ett gemensamt nät kan innebära och hur det tänkbart kan realiseras, kräver noggrann analys.

Det finns ett antal faktorer som medför tydliga skillnader mellan verksamhetsplanering och operativ verksamhet:

- *Mobilitet* – militär operativ verksamhet ställer betydande krav på mobilitet, vilket inte verksamhetsplanering gör på samma sätt.
- *Hantering av större informationsmängder* – vid verksamhetsplanering finns normalt mer omfattande datorresurser och datamängder att hantera, medan operativ verksamhet har större behov av snabba beräkningar och beslut.

- *Sekretessbelagd information* – spelar en avgränsad roll i fält men kan vara av central vikt vid verksamhetsplanering.
- *Enkelhet och robusthet kontra säkerhet* – fältmässiga situationer präglas av behov av enkelhet och robusthet medan verksamhetsplaneringsnivå främst har behov av säkerhet.
- *Skydd och verkan* – säkerhetsfokus vid verksamhetsplanering medför skyddsbehov medan verkan kan tvingas gå före skydd vid operativ verksamhet.
- *Riskvärdering* – i fält behövs robusta metoder för riskvärdering och med tanke på tidsbrist är automatiserade metoder av intresse. Verksamhetsplanering präglas däremot inte av samma tidskritiska perspektiv avseende riskvärdering.
- *Tidsperspektiv* – operativ verksamhet kräver snabba beslut och agerande medan verksamhetsplanering har längre tidsperspektiv.
- *Riktighet kontra sekretess* – i fält är riktighet av större vikt än sekretess. Likaså är det i fält av stor vikt att information är uppdaterad, vilket innebär behov av inhämtning av information. Vid verksamhetsplanering har sekretess större vikt.

Det kommande yrkesförsvaret kan påverka rollfördelningen och kopplingen mellan verksamhetsplanering och operativ verksamhet. Den militära organisationen kommer på ett annat sätt skilja krigsförbanden från administrationen och specialistroller kan tillkomma. Detta kan även innebära ändrade avvägningar och prioriteringar rörande informationssäkerhet.

Bra kommunikation mellan verksamhetsplanering och operativ verksamhet är av vikt, för att säkerställa hög informationssäkerhet och säkerställa förståelsen för informationssäkerhetsbehoven.

4.1.2 Samverkan

Samverkan med civila och militära aktörer har utvecklats till vardagsverksamhet, vare sig det är tal om samverkan med myndigheter, koalitionspartners eller andra. Detta innebär såväl möjligheter som utmaningar. Med avseende på informationssäkerhet behövs tydliga avvägningar, prioriteringar och kunskap om vilka samverkan sker med. Exempelvis medför olika sekretesspolicyer och hanteringssätt behov av väl utvecklade samverkansmetoder.

4.1.3 Säkerhetsbalans

Avvägning behövs mellan behov av sekretess, tillgänglighet, riktighet samt kostnader. Med rätt identifierat verksamhetsfokus underlättas sådan avvägning. Avvägningen kan även medföra sidoeffekter, som till exempel att ökad

tillgänglighet kan uppnås genom sekretessbelagd trafikinformation som försämrar motståndares möjligheter till att störa ut kommunikationsnäten.

Kunskap om olika aktörers behov, beteende och handlingsmönster är också av vikt för att nå en rimlig säkerhetsbalans. I samverkan med olika civila aktörer och koalitionspartners accentueras vikten av denna balansgång. Detta gäller även hantering av insiderproblematiken, där det kan noteras att samverkanssituationer komplicerar frågan om vem som utgör insider. Samverkan ger därmed nya möjligheter, men även nya utmaningar att hantera.

Ett ändrat perspektiv på säkerhet kunde skönjas i intervjuerna. Behovet av att aktivt beakta hotbild, operations- och insatsmiljö för att uppnå önskad effekt och säkerhet har blivit vanligare. Detta innebär att från att tidigare ha fokuserat på sekretess har även tillgänglighet fått ökad betydelse. Spårbarhet kommer samtidigt fram som en viktig aspekt av informationssäkerhet.

Distribuerad informationshantering ökar och medför andra behov vad gäller säkerhet och riskhantering. Situationen minskar rollen perimeterskydd kan spela men samtidigt kan centralisering ge mer ekonomisk drift eftersom man kan dra nytta av sin storlek. Försvarsmaktsinterna moln kan ge centralisering av drift, men distribuerad verksamhet och användning.

4.2 Hur objektbaserad säkerhet möjliggörs

Målsättningen med OBS är att ge ökad tillgänglighet med bibehållen sekretess, spårbarhet och riktighet. Detta åstadkoms genom att OBS tillför följande förmågor:

- Bibehålla objektens sekretess och riktighet i rörelse och vila oberoende av fysisk plattform.
- Bibehålla objektens sekretess och riktighet under användning.
- Möjliggöra spårbarhet för både användare och informationsägare.

Kravet på att OBS skall möjliggöra spårbarhet härstammar från Försvarsmaktens krav på att alla IT-system skall erbjuda denna funktionalitet (Försvarsmakten, 2004). Tidigare har spårbarheten oftast möjliggjorts av den infrastruktur som objekten har hanterats på men det är inte möjligt i OBS. Om OBS skall hantera hemliga uppgifter är spårbarheten ett lagkrav (SFS 1996:633).

Vidare måste OBS också kunna fungera autonomt eftersom Försvarsmaktens verksamhet innebär att uppkoppling inte alltid är möjlig. För att kunna leverera dessa förmågor bedöms OBS behöva omfatta ett antal funktioner och mekanismer som beskrivs nedan.

4.2.1 Sekretesskydd för objekt i rörelse och vila

För att kunna uppnå OBS måste ett objekt vara skyddat i sig självt för att förhindra obehörig tillgång till informationen. Troligen kan denna funktion åstadkommas genom kryptering då sekretesskyddet måste fungera även utanför betrodd hårdvara.

Krypteringsbaserade sekretesskydd för objekt i rörelse och vila hanteras inom forskningen för CBIS, kryptering, användningskontroll och informationsfokuserade nätverk.

4.2.2 Betrodd plattform

För att kunna skydda ett objekt under användning måste det isoleras från övriga processer i det aktuella IT-systemet. Detta innebär att den aktuella plattformen som exekverar objektet måste vara betrodd (Park och Sandhu, 2004).

Forskningen inom MLS och MIC presenterar flera möjliga metoder som är intressanta att utvärdera i samband med OBS.

4.2.3 Policy för användning

Policyn som reglerar användning är central för att avgöra vem som får använda ett objekt. Det måste också vara möjligt att förändra policyer under objektets livslängd. $UCON_{abc}$ kan användas som en grundmodell för att beskriva de policyer som utgör användningskontroll i OBS.

I forskningen inom CBIS presenteras möjliga lösningar på hur policyer kan bindas till objekt samt på hur de kan skapas och distribueras.

4.2.4 Verifierbara attribut

För att bevilja åtkomst till ett objekt är det kritiskt att på ett tillförlitligt sätt kunna verifiera de attribut som medger behörigheten. För att uppfylla de förmågor som OBS eftersträvar krävs endast ett verifierbart attribut. I OBS bör detta attribut med största sannolikhet utgöras av användaridentiteten.

Tidigare forskning inom CBIS och användningskontroll presenterar flera lösningar på hur attribut kan verifieras på ett tillförlitligt sätt.

4.2.5 Nyckelhantering

Om kryptering används för att bibehålla sekretessen behöver någon form av nyckelhantering ingå i OBS. Kiviharju (2010) redogör för flera möjliga metoder för nyckelhantering och utvärderar vilken som är lämpligast för CBIS. Denna kunskap kan återanvändas inom OBS.

Andra beskrivningar finns i forskningen kring användningskontroll, kryptering och informationsfokuserade nätverk.

4.2.6 Unikt identifierbara objekt

För att åstadkomma spårbarhet måste varje objekt i OBS vara unikt identifierbart och det subjekt som använder objektet säkert identifierat. Unika objekt gör det också möjligt för användaren att verifiera objektets ursprung och riktighet.

En annan central förutsättning för OBS är att objekt och deras metadata i form av policyer är oskiljaktigt bundna till varandra. Detta är inte detsamma som att metadata behöver följa med objektet utan det är tänkbart att metadata lagras på centrala servrar och att de binds till objektet via dess unika identitet. På så sätt gör unika objekt det möjligt att använda flera alternativa arkitekturer för att bygga OBS.

Unikt identifierbara objekt ingår som en del i forskningen kring användningskontroll, CBIS, kryptering och informationsfokuserade nätverk.

5 Diskussion

För att åstadkomma ett fungerande system för OBS måste ett antal tekniska och administrativa utmaningar hanteras.

5.1 Kryptering

Eftersom de krypterade objekten i OBS finns distribuerade uppstår problem med att byta nycklar och kryptosystem om det skulle behövas på grund av brister i kryptosystemet eller förlorade nycklar. Enligt gällande lagstiftning kan ett objekt vara hemligt i upp till 70 år (SFS 2009:400). En möjlig lösning på detta dilemma skulle vara att endast hantera objekt med korta sekretesstider.

Som det framkom ur intervjuer är det dock inte uppenbart att sekretess över längre tid är ett behov i fältmässiga situationer. Överhuvudtaget framkom att vikten av sekretess inte nödvändigtvis är så stor i fält, eftersom information snabbt blir inaktuell.

5.2 Användningskontroll

Det är av vikt att kontrollera vilka som skall få tillgång till objekt och vad dessa är behöriga att göra med objekten. Ett sätt att uppnå detta är att använda policyer men här föreligger flera utmaningar. För det första måste dessa på något sätt kopplas till respektive objekt. För det andra är det viktigt att kunna distribuera policyn så att systemet vet vad som gäller för just det specifika objektet. För det tredje måste det vara enkelt för ägaren till ett objekt att skapa relevanta policyer i samband med att objektet skapas och dessa måste kunna förändras vid behov.

Gamer, Völker och Zitterbart (2009) presenterar ett exempel på hur sådana policykontroller kan fungera genom att styra vilka nätverksnoder ett objekt får passera. En annan tänkbar kontroll är att styra vilka noder ett objekt får lagras på. $UCON_{abc}$ kan användas för att skriva policyer på ett bra sätt. Denna metod klarar av flera olika typer av åtkomstkontroll, bland annat rollbaserad och attributbaserad sådan.

I intervjuerna framkom att variationsrikedomen bland Försvarsmaktens verksamhet är stor, vilket policyer måste väga in. Såväl verksamhetsmiljö, hotbild, sårbarheter som former för samverkan kan variera. Alla dessa faktorer påverkar dessutom avvägningen mellan informationssäkerhetsegenskaperna sekretess, tillgänglighet och korrekthet. Exempelvis föreligger skillnader mellan insatsverksamhet och verksamhetsplanering vad gäller den systemkomplexitet som går att hantera. Eftersom nyckelhantering är komplext måste sådana metoder hållas enkla i fält, även om mer omfattande metoder kan vara acceptabla på verksamhetsplaneringsnivå.

Dessutom visade intervjuerna att det i fält är viktigt med flexibelt skydd för att tillåta avvägning mellan skydd och verkan. Detta kan exempelvis behövas för att hantera plötsliga förändringar i behörighetsbehovet, som kan uppstå om en befattningshavare försätts ur stridbart skick. Då måste det vara möjligt att förändra villkoren för behörighet så att den nya befattningshavaren får rätt, eller i alla fall en tillräckligt bra, åtkomst.

Kontinuerlig autentisering och auktorisation skyddar ett objekt under användning genom att ett antal villkor hos användaren kontrolleras. Exempel på villkor kan vara att ha ett visst skyddsprogram igång, att åtkomst efterfrågas vid en viss tidpunkt eller att användaren befinner sig på en viss geografisk plats. För att kunna lita på kontrollen av dessa villkor måste man i sin tur lita på den plattform som kontrollerar villkoren. Som framkom i intervjuerna är det då viktigt att sensorinformation som utgör indata till villkoren är korrekt och uppdaterad för att det ska gå att lita på de attribut som en användare anger för kontroll mot villkoren.

Det är också viktigt att objekt under användning kan skyddas från övriga processer på användarens dator vilket kan åstadkommas med en betrodd plattform. Om den betrodda plattformen utgörs av speciell hårdvara kan de behov som framkom i intervjuerna rörande enkelhet och robusthet som finns i fält försvåras. Om den betrodda plattformen däremot åstadkoms med mjukvara på en generell hårdvara, så är det en utmaning att åstadkomma hög assurans. Detta är ett problem som kvarstår att lösa. Det skulle även kunna tänkas att en mer begränsad form av tillgång ges om attribut inte kan verifieras mer än till viss del, för en mer dynamisk användningskontroll.

En annan utmaning är att välja villkor och sätt att beskriva dem. I ett tidigare FOI-projekt (Westerdahl, 2011) har attributbaserad åtkomstkontroll undersökts och en demonstrator som visar hur denna kan fungera har tagits fram. Denna kunskap utgör en lämplig startpunkt för villkorshanteringen i FOI:s fortsatta forskning inom OBS.

5.3 Samverkan

Försvarsmakten samverkar med en mångfald av aktörer och därför finns ett behov av att OBS underlättar samverkan, till exempel inom koalitioner. Även om motpartens kontroll av behörighet anses fullgod så uppstår ett översättningsproblem eftersom de attribut som används för behörighetskontroll troligen är annorlunda i sin utformning. Detta kan även vara ett problem vid kommunikation mellan olika säkerhetsdomäner inom samma organisation, men mildras troligen något av att attributen har en liknande struktur. För att underlätta samverkan inom koalitioner och mellan befintliga säkerhetsdomäner vore det önskvärt att utveckla bra metoder för hur samverkan mellan säkerhetsdomäner med olika format på attributen kan ske.

Om OBS uppnår ökad tillgänglighet med bibehållen sekretess, har den som säkerhetsmodell potential att i högre grad möjliggöra samverkan.

5.4 Autonomitet

Som det framkom i intervjuerna innebär Försvarsmaktens verksamhet att det inte går att förutsätta att en enhet hela tiden har kommunikation med omvärlden. Det kan till exempel röra sig om ett förband som iakttar radiotystnad eller en enhet som helt enkelt befinner sig i ett geografiskt område med begränsade kommunikationsmöjligheter.

Det framkom också i intervjuerna att behovet av tillgänglighet till information är mycket högt, speciellt för ledningssystem men till viss del även för fredstida kontorssystem. Även om normalläget för systemet är uppkopplat så måste OBS således inkludera tekniker som möjliggör autonomitet.

5.5 Relevans för Försvarsmakten

OBS bedöms vara intressant för Försvarsmakten eftersom möjlighet att åstadkomma högre tillgänglighet och flexibilitet med bibehållen sekretessnivå skulle kunna uppnås. En fullt utbyggd lösning gör det enklare att åstadkomma ett informationsövertag eftersom rätt information kan användas av rätt person vid rätt tillfälle.

6 Slutsatser och framtida arbete

I det här kapitlet presenteras de slutsatser som kan dras ifrån diskussionen i kapitel 5. Dessa slutsatser ligger sedan till grund för de förslag på framtida arbete som ges.

6.1 Slutsatser

Följande slutsatser drogs av materialet:

Försvarsmakten har behov av ökad flexibilitet och tillgänglighet

Det finns ett stort behov av att samverka med andra aktörer inom och utanför koalitioner. Form och innehåll i ett samarbete varierar mycket beroende på omständigheterna vilket gör behovet svårt att förutse. Dessutom är autonomitet ett viktigt behov inom Försvarsmakten.

Behovet av sekretess varierar inom Försvarsmakten

Det finns en stor variation vad gäller den tid som enskilda uppgifter behöver hemlighållas. Ledningssystem för insatser har typiskt ett kortare behov av sekretess i och med att tiden från planering till genomförande är kortare och information slutar ofta att vara känslig efter genomförande. Mer strategiska system och kontorssystem för utveckling har däremot ett större behov av att kunna skydda uppgifter över en längre tid.

Försvarsmakten har behov av att hantera kontorssystem

Försvarsmakten är inte enbart en insatsorganisation utan även en myndighet. Det innebär att vardagen för flera anställda innehåller interaktion med kontorssystem, till exempel för tidsrapportering och resebeställningar men även för utvecklingsarbete och kontakt med externa parter. Det gör att Försvarsmakten i flera avseende har samma behov av informationssäkerhet som andra myndigheter och företag.

OBS är tekniskt möjligt att åstadkomma med dagens teknik

Det är dock svårt att påvisa vilken assuransnivå en sådan lösning kan ge. Ur ett åtkomstperspektiv kräver lösningen betydande utnyttjande av tjänster i nätet och underhåll av metadata. Ur ett nyttjandeperspektiv krävs en plattform hos konsumenten som system- och informationsägaren kan lita på.

6.2 Framtida arbete

Även om OBS är tekniskt implementerbart så behövs vidare arbete för att kunna fastställa inom vilka gränser och till vilken assurans som säkerhetsmodellen kan användas. Inom ramen för projektet föreslås en framtida inriktning mot att identifiera en övergripande arkitektur, för att därefter undersöka vilka egenskaper som är kritiska för de ingående komponenterna.

7 Referenser

CCN, 2012, Content-centric networking, Parc, [online] <http://www.parc.com/services/focus-area/content-centric-networking/> [Kontrollerad 10 september 2012].

CCNx, 2012. [online] <http://www.ccnx.org/> [Kontrollerad 10 september 2012].

Försvarsmakten, 2004. Krav på säkerhetsfunktioner – Grunder, 10 750: 78976.

Försvarsmakten, 2008. FM CIO Chief Information Officer Strategi, Bilaga till HKV 09 100:74337.

Försvarsmakten, 2009. CIO Måldokument för Nät- och Informationsstruktur (NII), Bilaga till 09 100:64095.

Gamer, T., Völker, L. & Zitterbart, M., 2009. Differentiated security in wireless mesh networks, Wiley InterScience, [online] <http://www.interscience.wiley.com> [Kontrollerad 10 september 2012].

Harrington, A. & Jensen, C. D., 2003. Cryptographic access control in a distributed file system. *SACMAT*, pp. 158-165.

Jacobson, V., Mosko, M., Smetters, D. & Garcia-Luna-Aceves, J.J., 2007. Content-centric networking: Whitepaper describing future assurable global networks. Palo Alto, USA: Parc.

Kiviharju, M., 2010. Content-Based Information Security (CBIS): Definitions, Requirements and Cryptographic Architecture. Riihimäki, Finland: Defence Forces Technical Research Centre.

Kiviharju, M., (opublicerad) On multi-level secure structured content. Riihimäki, Finland: Defence Forces Technical Research Centre.

Lazouski, A., Martinelli, F. & Mori, P., 2010. Usage control in computer security: A survey. *Computer Science Review* 4 (2), pp. 81-99.

McGovern, S., 2001. Information Security Requirements for a coalition wide area network, Thesis in Naval Postgraduate School.

Müller, S., Katzenbeisser, S. & Eckert, C., 2009. Distributed Attribute-Based Encryption. *ICISC 2008*, vol. 5461, pp. 20-36.

NetInf, 2012. Network of Information, [online] <http://www.netinf.org> [Kontrollerad 10 september 2012].

Park, J. & Sandhu, R., 2004. The UCONABC Usage Control Model. *ACM Transactions on Information and System Security*, vol. 7, nr. 1, pp.128-174.

Riley, S., 2006. Mandatory integrity control in Windows Vista, Steve Riley on Security, [online] <http://blogs.technet.com/b/steriley/archive/2006/07/21/442870.aspx> [Kontrollerad 10 september 2012].

Sahai, A. & Waters, B., 2004. Fuzzy Identity Based Encryption. *IACR Cryptology ePrint Archive,* vol. 86.

SFS 1996:633. Säkerhetsskyddsförordningen.

SFS 2009:400. Offentlighets- och sekretesslag.

Shamir, A., 1984. Identity-based cryptosystems and signature schemes. *Advances in Cryptology – CRYPTO*, vol. 196, pp. 47–53.

SIS, 2007. HB 550, Terminologi för Informationssäkerhet. Utgåva 3. Stockholm: SIS Förlag.

Stihler, M., Olivo Santin, A., Calsavara, A. & Marcon Jr., A.L.,2009. Distributed Usage Control Architecture for Business Coalitions. *IEEE ICC 2009 proceedings.*

Westerdahl, L., 2011. Objekt- och tjänstebaserad säkerhet, FOI-R--3361--SE. Linköping, Sverige: FOI.

Zhang, X., Nakae, M., Covington, M.J. & Sandhu, R., 2008. Toward a Usage-Based Security Framework for Collaborative Computing Systems. *ACM Transaction on Information System Security,* vol. 11, nr. 1.

Zou, D., 2009. DVM-MAC: A Mandatory Access Control System in Distributed Virtual Computing Environment. Parallel and Distributed Systems (ICPADS), 15th International Conference. Shenzhen, Kina dec 2009.

Bilaga A: Intervjuguide

Inledning

Inom ett projekt vid FOI rörande Objektbaserad säkerhet genomför vi en intervjustudie under våren 2012.

Intervjustudien avser göra en förenklad kartläggning av informations-säkerhetsbehov inom Försvarsmakten, särskilt med avseende på den variationsrikedom av operativa situationer som militära enheter kan hamna i. Centralt i detta är att få en uppfattning av huruvida beroendet av fast informationsinfrastruktur och fysiska maskiner kan tänkas minska. Därmed berörs även frågan huruvida informationsobjekt kan tänkas skydda sig själva och vilka konsekvenser, möjligheter och begränsningar detta kan bedömas innebära.

Är inspelning av intervjun ok?

Bakgrund

Vilken är din nuvarande tjänst?

Kan du kort beskriva din huvudsakliga arbetsuppgift?

Vilken erfarenhet har du av arbete som inbegriper informationssäkerhet?

Scenarion

Som utgångspunkt för intervjuerna har vi tagit fram en enkel tabell över ledningsnivå relativt strid och patrullering.

Hur väl täcker tabellen olika kategorier av operativa militära situationer? Beskriver tabellen variationsrikedomen tillräckligt väl (bredd, upplösning)?

- Vilka situationsbeskrivningar har inte kommit med i tabellen?

Vilka övergripande reflektioner kan göras om sekretess- och tillgänglighetsbehov i de olika situationer som tabellen beskriver?

Vilka övergripande reflektioner kan göras om behov av korrekta data (information), dvs. dataintegritet, i de olika situationer tabellen avser övergripande beskriva?

/Här kan eventuellt olika mera detaljerade scenarion presenteras för respondenten, om så behövs./

Dagens informationssäkerhetsbehov

Vilken variationsrikedom har militär verksamhet idag?

- Vilken variation ger detta avseende informations-säkerhet och informationssäkerhetsbehov? Hur hanteras detta idag?

- Vad ytterligare behövs för att hantera detta?

I vilken mån hanteras data och information centralt respektive distribuerat? Hur påverkar detta hanteringen av informationssäkerhet och prioriteringen mellan sekretess, tillgänglighet och korrekthet?

Framtida informationssäkerhetsbehov

Vilken variationsrikedom bedömer du att militär verksamhet får i framtiden?

- Vilken variation ger detta avseende informations-säkerhet och informationssäkerhetsbehov? Hur kan detta hanteras?

I vilken mån kommer data och information hanteras centralt respektive distribuerat? Hur påverkar detta hanteringen av informationssäkerhet och prioriteringen mellan sekretess, tillgänglighet och korrekthet?

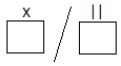
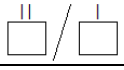
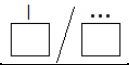
Är det rimligt att förvänta sig en utveckling där informationsobjekt i ökande grad inhämtas från olika källor och vägs ihop till t ex en lägesbild

- Är detta en önskvärd utveckling?
- Vilka möjligheter och begränsningar ger en sådan utveckling?
- Vilken utveckling medför detta relativt koppling till fysiska maskiner och infrastruktur?

Sammanfattning

Tack för din medverkan

Bilaga B: Militära typsituationer

	Krig/strid	Fred/patrull
Hög nivå/ledning 		
Mellannivå 		
Låg nivå 		

 Brigad

 Bataljon

 Kompani

 Pluton

 Grupp