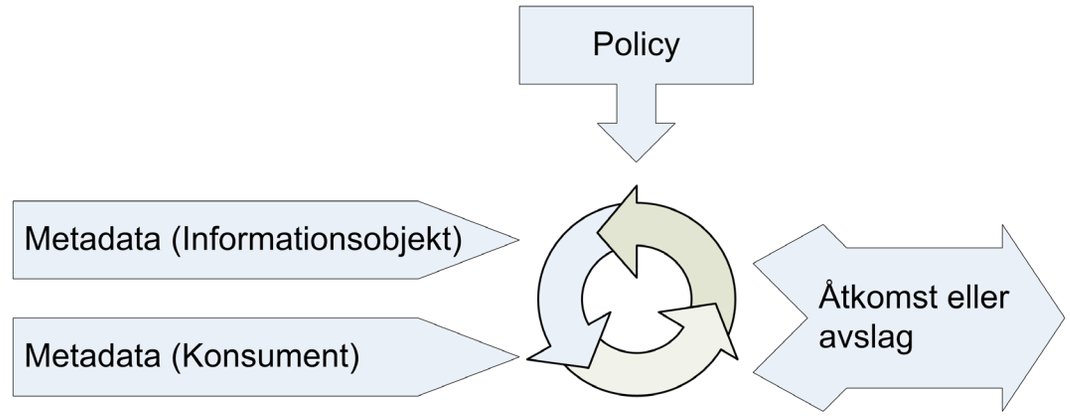
Objekt- och tjänstebaserad säkerhet

Slutrapport

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
Informationssystem
164 90 Stockholm

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

www.foi.se

FOI-R--3361--SE
ISSN 1650-1942

Användarrapport
December 2011

Informationssystem

Lars Westerdahl

Objekt- och tjänstebaserad säkerhet

Slutrapport

Titel	Objekt- och tjänstebaserad säkerhet - Slutrapport
Title	Object- and service-oriented security – Final report
Rapportnr/Report no	FOI-R--3361--SE
Rapporttyp /Report Type	Användarrapport / User Report
Månad/Month	December/December
Utgivningsår/Year	2011
Antal sidor/Pages	39 p
ISSN	ISSN 1650-1942
Kund/Customer	Försvarsmakten
Projektnr/Project no	E5055
Godkänd av/Approved by	Magnus Jändel

FOI, Totalförsvarets Forskningsinstitut
Avdelningen för Forskningsstöd

164 90 Stockholm

FOI, Swedish Defence Research Agency

SE-164 90 Stockholm

Sammanfattning

Projektet *Objekt- och tjänstebaserad säkerhet* har undersökt om säkerhetsfunktioner kan erbjudas som tjänster. Syftet med en tjänsteorientering är att skapa flexiblare system vilka lättare och snabbare kan anpassa sig efter nya förhållanden, till exempel när medlemmar i en koalition tillkommer eller lämnar koalitionen.

Teknikutvecklingen under projektets gång har varit snabb, vilket har inneburit att en hel del säkerhetsfunktioner i dagsläget kan erbjudas som molntjänster. Ur ett försvarsperspektiv är dock inte publika molntjänster aktuella i nuläget. Däremot kan interna säkerhetsfunktioner mycket väl kunna fungera som tjänster och därmed bidra till en mer konsistent och förutsägbar IT-utveckling.

Under projektets gång har begreppet objektbaserad utveckling fått en allt större betydelse. Tjänsteorientering av säkerhetsfunktioner bedöms vara en metod för att sprida ut säkerhetsfunktioner och därmed öka tillgängligheten för informationsobjekt.

Nyckelord: IT-säkerhet, Informationssäkerhet, Tjänsteorientering

Summary

The project *Object- and service-oriented security* has explored the possibilities for presenting security functionality as services. The purpose with service orientation is to create more flexible systems, which can adapt to new environments and situations easier and quicker, for instance when coalition partners enters or leaves the coalition.

The development in the internet community during the lifetime of the project has been fast. As a consequence, some security functionalities are today offered as cloud services. Public cloud services are not yet mature from a defence point of view. However, offering security functionalities as internal services may be beneficial. It could provide a more consistent and predictable development.

During the lifetime of the project, there has been a shift in focus towards object-based security. Service orientation of security functionality has been deemed a way forward to distribute security functionalities and thus increase the availability of information objects.

Keywords: IT-security, information security, Service-oriented architecture

Innehållsförteckning

1 Inledning

Försvarsmakten har som målsättning att upprätthålla en expeditionär förmåga. En sådan förmåga förutsätter att förband snabbt skall kunna förflyttas en längre sträcka och ibland även att kunna agera självständigt under en längre tid (Flygelholm et al., 2008, s.8). Sannolikt sker dock expeditionära insatser i koalition med andra nationer vilket ställer krav på förmågan att samverka (NNEC FS, 2005).

Samverkan kan ske på fler sätt och på fler nivåer. För att uppnå ett effektivt samarbete är det sannolikt att information behöver utbytas. Det kan också innebära att tjänster kan tillgängliggöras för andra koalitionsmedlemmar under en begränsad tid. För att möjliggöra utbyte och delning måste lednings- och informationssystem vara flexibelt uppbyggda för att kunna hantera nya användare av systemet efterhand som behov uppstår.

Informations- och ledningssystem har hitintills byggts med begränsad informationsdelningsförmåga. De förutsättningar för vilket ett system ursprungligen skapades kan ha förändrats även om systemet fortfarande är i bruk. Detta är särskilt begränsande för säkerhetsfunktioner, då de har som huvuduppgift att reglera åtkomst till resurser. Det gör att säkerhetsfunktioner ofta har svårt att hantera strukturella förändringar avseende vilka system de skall stödja. Informationsdelning över systemgränser och då särskilt säkerhetsdomäner har varit, och fortfarande är, problematiskt. Tjänsteorientering av säkerhetsfunktioner inom informations- och ledningssystem är en ansats för att centralisera administration och därmed snabbare kunna få genomslag för förändringar avseende behörigheter. Förhoppningen med centraliserad administration är även att dialog och behörighetshantering över systemgränser underlättas.

I CIO:s måldokument (CIO, 2009) anges att säkerhetslösningar skall sträva mot objektbaserade säkerhetslösningar, det vill säga säkerhetslösningar vilka primärt fokuserar på att skydda informationsobjekt. Centraliserade och tjänsteorienterade säkerhetsfunktioner stödjer en infrastruktur för objektbaserad säkerhet. Med exempelvis en auktorisationstjänst kan en konsument vända sig till auktorisationstjänsten för att få behörighet till ett informationsobjekt. På så sätt fokuserar säkerhetslösningen på informationsobjektet och inte dess ursprungliga lagringsplats eller vägen däremellan. Projektet har följt den akademiska och kommersiella utvecklingen inom området objektbaserad säkerhet.

Inom projektet sker även ett deltagande i *IST-096 Informations Assurance / Cyber Defence Research Framework* vilket är en forskningsgrupp inom NATO. Forskningsgruppens arbete syftar mot att ta fram specifikationer av nödvändiga

förmågor för att bedriva cyberförsvar (eng. cyber defence) samt säker informationsöverföring (eng. secure information sharing).

1.1 Frågeställningar

Projektets huvudspår har varit inriktat mot tjänsteorienterad säkerhet. Inom detta område har tre övergripande frågeställningar följt projektet. Dessa är:

I. Vilken säkerhetsfunktionalitet kan hanteras som en tjänst?

II. Vilken säkerhetsfunktionalitet måste finnas och hanteras lokalt?

III. Hur kan en förmåga att välja säkerhetsnivå beroende på uppgift skapas, det vill säga beroende på vilka säkerhetsegenskaper som kan levereras som tjänster borde det vara möjligt att dynamiskt skapa olika säkerhetsprofiler efter behov?

Parallellt med huvudspåret har även projektet haft en delfrågställning i syfte att följa utvecklingen inom området objektbaserad säkerhet.

IV. Vilka egenskaper och vilken prognos har existerande tekniker för objektbaserad säkerhet?

Tolkningen av frågeställningarna har under projektets gång gått mot att mer och mer kunna hantera säkerhet runt informationsobjekt än om tjänster.

1.2 Avgränsningar

I dokumentet behandlas tjänster i den betydelse de har inom tjänstebaserade arkitekturer för IT-system. Tolkningen av tjänsteorientering avgränsas till den som ges av *Organization for the Advancement of Structured Information Standards* (2005).

Själva urvalet av tjänster begränsas till de säkerhetsfunktioner som definieras i dokumentet *Krav på säkerhetsfunktioner* (Försvarsmakten, 2004).

1.3 Rapportstruktur

Rapporten struktureras enligt följande. Kapitel två beskriver det verksamhetsmässiga problemområdet ur vilka säkerhetsproblemen identifieras. Kapitel tre presenterar en sammanfattning över hur IT-säkerhetsområdet har utvecklats under projekttiden relaterat till problemområdet. Kapitel fyra till sex behandlar huvudfrågeställningarna inom projektet. I kapitel fyra avhandlas vilka säkerhetsfunktioner som kan lämpa sig för att erbjudas som en tjänst. Kapitel fem beskriver hur en tjänst kan användas för att skapa dynamisk åtkomst till information men stöd av en tjänstebaserad åtkomstkontroll. Kapitel sex

presenterar utvecklingen inom området objektbaserad säkerhet. Kapitel sju och åtta sammanfattar arbetet och beskriver identifierade faktorer för fortsatt arbete. Kapitel nio är rapportens referenslista, medan kapitel tio utgör projektets publikationslista.

2 Problemområde

En av Försvarsmaktens uppgifter är att utveckla en expeditionär operativ förmåga. Med denna förmåga kan Sverige stärka sitt försvar genom att minska eller neutralisera konflikter innan de når våra gränser. Försvarsmakten förväntas inte kunna lösa ut denna uppgift på egen hand utan ett samarbete med andra nationer, myndigheter och organisationer förutsätts (Flygelholm, Norlander & Hansson, 2008).

För att samarbeta på ett effektivt sätt innebär utbyte av information och ibland även tjänster i form av stödsystem. Att koppla samman system är inte nödvändigtvis tekniskt svårt så länge de kommunicerar på ett någorlunda standardiserat sätt. Problem uppstår snarare när varje nation skall säkerhetsställa att kommunikationen sker på ett tillförlitligt sätt och inte inverkar skadligt på den egna nationens intressen eller system.

Problemet med att hantera verksamhetsmål, såsom dela infomationtillgångar, med andra medlemmar i en mission, och nationella säkerhetsbestämmelser har pågått länge, men har kanske blivit tydligast under missionen i Afghanistan. *Afghan Mission Net* skapades utifrån behovet av att kunna kommunicera mellan medlemmar inom koalitionen[1]. Problemen med att dela information återfinns även i mindre skala inom Försvarsmakten när interna system vill kommunicera med omvärlden.

En lång livslängd för ett IT-system medför en högre risk att systemen vid något tillfälle används på ett sätt eller i en miljö som inte förutsågs när systemet kravställdes. Livscykeln för system inom Försvarsmakten tenderar att vara lång. Detta verkar även gälla ledningssystem även om livslängd är kortare än för andra typer av system. För att ledningssystem skall kunna anpassas för nya uppgifter och nya samarbetspartners måste dessa system, och dess stödsystem, vara uppbyggda med en hög grad av flexibilitet i åtanke. Andra påverkansfaktorer för behov av flexibla system är att värdet av den information systemen skyddar varierar över tiden vilket gör att rätten till åtkomst kan variera.

2.1 Koalitionsparters

Det går inte i förväg säga vem eller vilka Försvarsmakten kommer att samarbeta med i framtida koalitioner. Det är inte ens möjligt för NATO[2]-länder att i förväg vara säkra på den frågan. Koalitioner uppstår där det finns ett problem som flera nationer har intresse att lösa, oavsett om det innebär att skapa nya koalitioner eller om befintliga samarbeten kan stärkas.

[1] http://www.nc3a.nato.int/news/Pages/20100801-AMN-approval.aspx (2011-11-28)
[2] North Atlantic Treaty Organisation, NATO.

De koalitioner Sverige deltagit i på senare år med insatta förband har i huvudsak varit ledda av NATO under ett FN-mandat. Sverige ingår även i en av EU:s Battlegroups. Varken NATO eller EU är hårt sammansatta grupperingar. Medlemsländerna kan vara anslutna till enbart NATO eller enbart EU, likväl som båda två samtidigt. Även inom en organisation som NATO kan kommunikationsförmågan variera då medlemsnationerna kan ha nationella särintressen eller förmåga till att leva upp till en gemensam NATO-standard.

Behovet av att kunna kommunicera en mission sträcker sig ofta även utanför den militära organisationen en nation deltar med. Myndigheter i värdlandet för missionen, icke-statliga organisationer samt ibland även företag kan vara exempel på enheter vilka tillfälligt kan behöva ingå i ledningssystemen.

NATO och EU är i sammanhanget stabila koalitioner. Det som gör dem stabila är att de är skapade med långsiktiga mål i åtanke och inte för att lösa ett kortsiktigt problem. Oroshärdar eller problem kan dock uppstå med ingen eller kort förvarning och de behöver inte alltid vara väpnade. Större olyckor och naturkatastrofer kan även ligga till grund för att Försvarsmakten behöver samarbeta med andra nationer och organisationer. I de här fallen är förberedelsetiden mycket kort.

Från ovanstående resonemang inses att det är svårt att förutse vilka system och vilka parter Försvarsmakten skall kunna kommunicera med. Denna slutsats har dragits av flera länder vilket har resulterat i ett stort intresse att skapa ledningssystem som bygger på öppna eller vedertagna industristandarder.

2.2 Informationens och systemens skyddsvärde

Information har olika värde för olika användare vid olika tillfällen. Tillgången till information kan ibland begränsas av att information finns på fysiskt åtskilda nätverk, men sekretess är det vanligaste anledningen till att åtkomst begränsas. En sekretessbedömning är visserligen bara tillfällig ur det perspektivet att en ny bedömning görs när informationen efterfrågas igen. Men det kan finnas andra aspekter som påverkar nyttan med att få tillgång till information. I IT-säkerhetssammanhang används ofta kombinationen sekretess, integritet och tillgänglighet[3]. Som nämnt ovan, så är sekretess den vanligaste bedömningsgrunden. Det kan dock finnas tillfällen då integritet och tillgänglighet skulle kunna vara av ett större verksamhetsvärde eller mer kostnadseffektivt. Information som delas med andra myndigheter över öppna system får inte vara

[3] Från eng. confidentiality, integrity och availability.

inklassade i någon informationssäkerhetsklass eller sekretessklassificerad[4]. Riktigheten i innehållet kan dock vara av större betydelse, vilket innebär att mekanismer för att bedöma informationens korrekthet får större betydelse. Behov av tillgänglighet skulle kunna ses från två håll. En användare som är behörig till en handling är, om enbart sekretess beaktas, lika behörig oavsätt varifrån eller när handlingen begärs. Genom att föra in andra variabler, såsom geografisk position, skulle åtkomst kunna varieras beroende på varifrån handlingen begärs. Om handlingen begärs ifrån användarens dator och dator är uppkopplad via arbetsplatsens lokala nätverk erhålls åtkomst. Begärs samma handling från användarens dator men via en virtuell tunnel från någon okänd fysisk plats, till exempel på ett tåg, skulle åtkomsten kunna begränsas. Den fysiska platsen från vilken användaren begär åtkomst av handlingen är en del av skyddet av handlingen.

Att använda en geografisk referens i åtkomstbeslutet vara var ett sätt att strama åt skyddet av en handling vilket skulle medföra en mer dynamisk åtkomstkontroll. Ett annat sätt att se på åtkomstkontroll är att platsen som användaren begär åtkomst ifrån faktiskt skulle öka behovet och därmed ge tillfällig behörighet. Ett exempel som skulle kunna visa på detta är en patrull som färdas längs en vägsträcka. Patrullen är insatt i de hot och risker som var kända vid avfärd. Längs vägen passerar patrullen ett område med misstänkt fientlig befolkning vilka står under uppsikt av ett annat spaningsförband. Patrullen har inte i normalfallet rätt att ta del av spaningsrapporter från förbandet men i den här situationen kommer patrullen finnas på en plats där de direkt påverkas av det förbandet kan observera. Närhet till informationsinnehållet skulle då kunna ge en tillfällig behörighet som tas bort så fort patrullen passerat området.

Än så länge har bara information i form av handlingar benämnts, men förutsättningarna är likvärdiga för systemfunktioner. Som exempel skulle tillgången till en specifik sensor kunna tas. En patrull får tillgång till sensorns informationsflöde (eller tolkningen av informationsflödet) så länge uppdraget pågår, men åtkomsten upphör när uppdraget är slutfört.

Ett tydligt steg mot att öka tillgängligheten av information tog Chief Information Officer (CIO) för Department of Defense, USA, i och med beskriv inriktning för informationshantering i *Department of Defense Net-Centric Data Strategy* (Department of Defense, 2003) och anammades av NATO i *NATO Network Enabled Capability Feasibility Study* (NATO Consultaion, Command and Control Agency, 2005). I dokumentet beskrivs en övergång från ”process, exploit, and disseminate” till “post before sharing”. Med detta avses att direkt

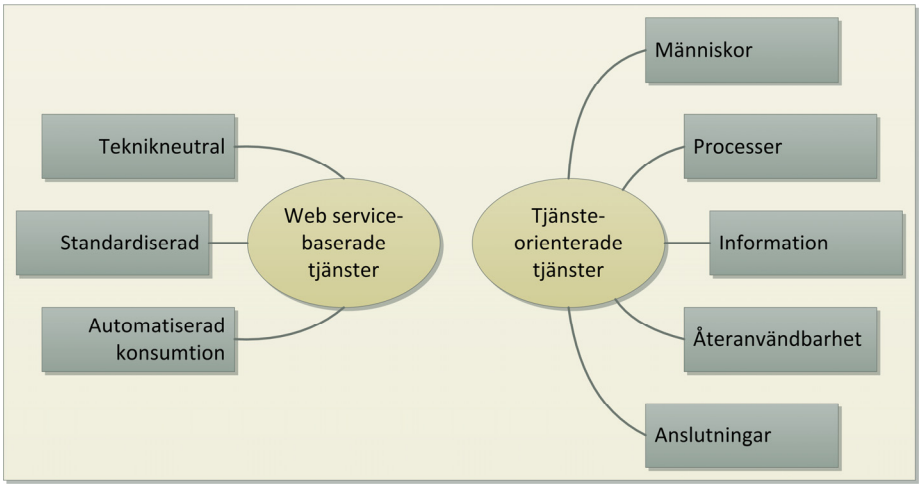
[4] Information som innehåller försvars- eller utrikessekretess skall vara tilldelad en informationssäkerhetsklass (HEMLIG/RESTRICTED, HEMLIG/CONFIDENTIAL, HEMLIG/SECRET, eller HEMLIG/TOP SECRET. Information som innehåller sekretess men som inte är försvars- eller utrikessekretess kallas sekretessklassificerad.

göra information tillgänglig via ett delat lagringsutrymme. På så sätt kan informationen användas av den som behöver, förstår och är behörig till det delade lagringsutrymmet betydligt snabbare än om informationen först skall hanteras av flera instanser innan den görs tillgänglig.

2.3 Tjänsteorienterad arkitektur

Begreppet tjänsteorienterad arkitektur (eng. Service Oriented Architecture, SOA) har vuxit fram ur ett behov av att göra funktioner tillgängliga på ett mer flexibelt sätt. En tjänst är någon form av funktionalitet vilken tillhandahålls av en systemägare, till exempel att få aktuell temperatur på en given plats. En intern funktion behöver endast vara känd och tillgänglig för dem som tillverkar applikationer som använder funktionen, men om funktionen skall exponeras som en tjänst tillgänglig för användare måste funktionen synliggöras på ett lämpligt sätt. En tjänst måste vara synlig, möjlig att kommunicera med samt ge någon form effekt hos den som använder tjänsten (Organization for the Advancement of Structured Information Standards, 2006). Synlig kan innebära sökbar för användare men det kan också vara att tjänsten görs synlig för den som är behörig. En synlig tjänst måste även vara tillgänglig vilket innebär att tjänsten skall kunna användas av den som ser densamma. Bara för att en tjänst är synlig innebär det inte att alla har rätt att använda tjänsten. Med tjänstekonceptet kommer även policys vilket innebär att det är den som producerar tjänsten som sätter nyttjanderegler. Med effekt avses att användaren skall få ut ett mätbart resultat från tjänsten, till exempel information i retur eller förändring av bifogade entiteter.

En teknologi som följt den tjänsteorienterade utvecklingen är så kallade *web services*. Även om web services inte helt och hållet inbegriper vad tjänsteorientering är så har det fångat mycket av tjänsteorienteringens egenskaper. Funktionalitet erbjuden som en web service måste vara tekrikneutral i betydelsen att mottagaren inte skall tvings till att använda något proprietärt format. Grundläggande för web services är standarder. Meddelande skickas i standardiserade format vilka, enligt tidigare, inte får vara kopplade till en viss teknologi. Utvecklingen inom bland annat web service har lett till en bred utveckling av extended markup languages protokoll, vanligare kallade XML-protokoll. De vanligaste protokollen inom web services är *Simple Object Access Protocol (SOAP)*, *Web Service Descripition Language (WSDL)* samt *Universal Description Discovery and Integration (UDDI)*. SOAP är ett protokoll som bär den efterfrågade informationen från producent till konsument, medan WSDL är en guide som anger hur förfrågningar skall vara formaterade samt hur svar tas emot. UDDI är web servicesystemets gula sidor vilket innebär att det är UDDI som annonserar ut tjänsterna för användare.



Figur 1: Egenskaper på web services och tjänsteorienterade system.

Det som framför allt avgränsar web services inom den tjänsteorienterade sfären är att web services är teknikorienterat. Huvudsyftet med web service är att skapa en kommunikationsmöjlighet mellan en producents och en konsuments system. Tjänsteorienteringen har ett större omfång och kan beskrivas ur perspektiven människor, information och processer (IBM, 2007). Utöver detta tillkommer även egenskaper som återanvändbarhet och anslutningsmöjlighet (Figur 1).

3 Utveckling inom säkerhetsområdet

IT-säkerhet har traditionellt i stort handlat om att identifiera gränser i syfte att förhindra obehörig åtkomst samt att övervaka att informationsflödet över gränsen följer givna riktlinjer. Men IT-säkerhet betyder olika saker för olika delar inom en organisation och de olika delarna kan ha väldigt olika mål med vad säkerheten skall åstadkomma.

På en hög nivå är IT-säkerhet kopplat till verksamhetsmål. System skall fungera och vara tillförlitliga även under påfrestningar. Men här finns även en tydlig balansgång mellan när tillgängligheten är bra och när IT-säkerhet blir en belastning för den egna verksamheten genom minskad tillgång. På en lägre nivå är IT-säkerhet mer teknikorienterat. Ur ett tekniskt perspektiv så uppnås IT-säkerhet genom beprövade säkerhetsfunktioner, det vill säga att IT-säkerhet uppnås genom att uppfylla ett tekniskt mål (Hafner & Breu, 2009, ss.6).

Efterhand som internetteknologin har mognat har allt fler försökt se vilka nya möjligheter publikt sammankopplade datorsystem kan ge för verksamheten. Utvecklingen på tekniksidan drivs av tillgänglighet och har gått fort, medan säkerhetssidan, vilken motiveras av avgränsning, har haft svårt att hänga med (Peterson, 2009). Innovationer som har ökat interaktionsförmågan för webbaserade applikationer har kommit ersatts allteftersom nya innovationer uppkommit. Detta har medfört att säkerhetslösningar för webbplattformen aldrig hunnit mogna och anpassa sig efter den nya tekniken. Det kan i vissa fall även finnas en konflikt mellan vad som i en värld med penna och papper har räknats som säkert och vad detta motsvarar i en digital värld.

Informationsutbyte är kritiskt för samarbete mellan organisationer. Mycket energi har lagts ner, och görs fortfarande, på att finna vägar för ett tillförlitligt informationsutbyte, både nationellt och internationellt. Nationellt har nyttjandet av informationsteknologi inom verktyg för samarbete fört framåt, bland annat genom arbetet med Försvarsmaktens Ledningssystem, FMLS. Motsvarande satsningar görs även i flera länder. NATO försöker ha en sammanhållande målbild för vad som bör uppnås genom arbetet med NATO Networking Enabling Capabilites, NNEC. Det praktiska arbetet med NNEC har resulterat i en teknisk arkitektur, *NATO Consultaion, Command and Control Technical Architecture (NC3TA)*, där bland annat informationsutbyte mellan nationer och organisationer inom och utanför en mission beskrivs i fyra scenarier. Informationsutbytet sker via Internet Exchange Gateways, IEG. Dessa gateways får en nyckelroll när det gäller säkerhetsmässiga kontroller av information till och från respektive nation eller mission. De flesta NATO-anslutna länder bedriver även utveckling av egna IEG:er.

Den interoperabla förmågan implementeras stegvis, vilket gör att säkerhetsfunktionalitet initialt fokuserar på skydda missionsnätet. Det framgår

dock att målsättningen med säkerhetsfunktionerna skall vara att logiskt kunna separera datamängder och användare efter behov. Traditionellt har detta genomförts genom fysisk separation men på grund av tillgänglighetskrav och kostnader för parallella system anses inte längre den vägen vara effektiv eller ekonomisk.

Försvarsmaktens CIO uttrycker en liknade vilja i Måldokument för Nät- och Informationsinfrastruktur genom målsättningen ”En och endast en gemensam nät- och informationsinfrastruktur”. Ett sådant nät är informationsorienterat jämfört med dagens mer systemorienterade nät. Säkerhet uppnås genom att en användare litar på källans system och att kommunikationen mellan källan och det egna systemet skyddas. I ett informationsorienterat nät måste tilltro till informationen kunna åstadkommas baserat på informationsobjektet själv. Därmed skulle informationen kunna komma till konsumenten av informationen från en annan avsändare än producenten, men konsumenten skall fortfarande kunna verifiera riktigheten.

En säkerhetsmodell vilken fokuserar på informationsobjekt kräver om inte nya säkerhetsfunktioner så i alla fall ett modifierat sätt att se på säkerhet. Redan i nuvarande säkerhetsmodell behöver information märkas så att en kontrollfunktion, till exempel en gateway, kan verifiera om informationen får lämna aktuell säkerhetsdomän. När väl informationen passerat gatewayn har producenten ingen kontroll över informationen längre. Inom projektet Objekt- och tjänstebaserad säkerhet benämns informationsmodellen som fokuserar på informationsobjekt för Objektbaserad säkerhet. Målbilden med objektbaserad säkerhet är att kunna hantera tillgång och nyttjande av informationsobjekt både inom och utanför den egna säkerhetsdomänen.

4 Säkerhet som en tjänst

De två första huvudfrågorna för projektet (I och II) svarar indirekt på varandra och kommer därför att presenteras samtidigt.

4.1 Säkerhetsfunktion som en tjänst

I stycke 2.3 beskrevs i grova drag uppbyggnaden av en tjänsteorienterad arkitektur. En konsument av en tjänst, vare sig det är en säkerhetsfunktion eller någon annan funktion, har sällan någon uppfattning om var eller hur tjänsten produceras. Det konsumenten är intresserad av är tillgänglighet samt den effekt tjänsten har för konsumentens system. Sannolikt gör inte ens konsumenten några aktiva val när det gäller nyttjandet av säkerhetsfunktionalitet, annat än att tillhandahålla autentiserings- och behörighetsinformation.

För en systemägare får tjänstebaserade säkerhetsfunktioner en större påverkan. Precis som för konsumenten är tillgänglighet viktigt men en systemägare måste även visa att IT-systemet uppfyller de krav på säkerhetsfunktioner som ställs i *Krav på säkerhetsfunktioner* (Försvarsmakten, 2004). För att kunna utnyttja tjänstebaserade säkerhetsfunktioner måste produktägaren av IT-systemet få någon form av garanti för att säkerhetstjänsten kan leverera den utlovade tillgängligheten, samt visa att IT-systemet inte försätts i ett känsligt tillstånd om tjänsten skulle haverera. Även om Försvarsmakten generellt inte har tjänstebaserade säkerhetsfunktioner i dagsläget finns det redan funktioner som påminner om detta. Försvarsmaktens virusskydd är ett centralt hanterat system där uppdatering och övervakning sker utanför de IT-system som använder tjänsten. Traditionella säkerhetsfunktioner som är lokalt implementerade är alltid åtkomliga för IT-systemet. Det samma gäller för uppslagstjänster. Förs resonemanget mot objektbaserad säkerhet kan det vara så att säkerhetstjänster, till exempel en åtkomstserver, inte är känd för konsumenten. I så fall måste informationsobjektet innehålla information som pekar ut rätt åtkomstserver. Avslutningsvis måste tjänsten tillföra samma effekt på IT-systemet som en lokalt implementerad säkerhetsfunktion.

En säkerhetsfunktion som är synlig och tillgänglig för det IT-system som behöver funktionaliteten, samt ger den effekt på IT-systemet som förväntas har goda chanser att fungera som en tjänst.

4.2 Säkerhetsfunktioner

I *Krav på säkerhetsfunktioner* (Försvarsmakten, 2004) tas sju säkerhetsfunktioner upp; behörighetskontroll, säkerhetsloggning, skydd mot röjande signaler, skydd mot obehörig avlyssning, intrångsskydd,

intrångsdetektering samt skydd mot skadlig kod. Dessa säkerhetsfunktioner har utgjort bedömningsgrunden för analys av vilka säkerhetsfunktioner som kan lämpa sig som tjänst.

4.2.1 Behörighetskontroll

Autentisering

Autentisering sker i flera led. Initialt är det en lokal process när användaren autentiserar sig mot den dator denne sitter vid. Den lokala inloggningen kan kopplas samman med en nätverksinloggning i de fall datorn är ansluten till ett nätverk. Därefter kan autentisering ske mot enskilda system på eller utanför nätverket.

En användare måste kunna genomföra den initiala autentiseringen lokalt då det inte alltid är säkert att en dator är uppkopplad mot ett känt nätverk. För en nätverksansluten dator är dock tjänsteanpassning ganska vanligt. Ett IT-system kan verifiera användare och andra IT-system gentemot en katalogtjänst, vilket typiskt är en nätverksresurs. Det som är begränsande för en katalogtjänst är till vilken grad produktägaren är villig att integrera användarkatalogen i det IT-system som finns på nätverket..

Auktorisering

Auktorisering är en funktion som mycket väl lämpar sig för att användas som en tjänst. Det finns dessutom stora vinster med att centralisera auktoriseringsbeslutet. Med ett centralt auktoriseringssystem får förändringar ett snabbare genomslag i det IT-system som nyttjar tjänsten.

4.2.2 Säkerhetsloggning

I ett modernt IT-system loggas en stor uppsättning händelser. Det kan ske på lokal nivå i ett enskilt IT-system och på en central nivå där loggar från underliggande IT-system samlas in för analys. Beroende på vad systemägaren vill uppnå med loggningen loggas olika mängd med händelser, särskilt i ett centralt system. Om syftet med loggningsfunktionen är att identifiera hot eller felaktigheter behövs en rätt så detaljerad loggningsdata från IT-systemen. Ett sådant system skulle sedan kunna larma en administratör om fel eller misstänkta händelser uppdagas. Skulle syftet med loggfunktionen vara att kartlägga händelser i efterhand räcker det att en mindre mängd loggar skickas till den centrala loggningsinsamlingen. Syftet med insamlingen är att skapa en bild över hur en användare har rört sig mellan olika IT-system. Därefter kontrolleras lokala loggar på aktuella system.

Lagring, arkivering, analys och hantering av larm är loggningsfunktioner som skulle kunna erbjudas som en tjänst.

4.2.3 Skydd mot röjande signaler

Elektronisk utrustning utstrålar energi när den strömsätts. Det innebär att det i vissa fall är möjligt att avlyssna en maskin genom att mäta den strålning maskinen alstrar. Skyddsåtgärder för att minska eller dölja strålning är helt och hållet kopplat till den fysiska maskinen och dess omgivning.

4.2.4 Skydd mot obehörig avlyssning

Skydd mot avlyssning sker i huvudsak genom att använda kryptering. En fil kan krypteras för att sedan kunna skickas över en öppen kanal, alternativt kan en krypterad kanal skapas för att skydda trafiken som löper i kanalen. Kryptering kan ske på flera nivåer i nätverksstacken, eller ovanför om det är ett filkrypto. Som en grundregel när det gäller kryptering är att krypteringen skall ske nära den oskyddade källan. På så sätt minimeras risken för avlyssning innan krypteringen är slutförd. Att skapa en tjänst för själva krypteringsförloppet skulle motsäga denna regel. Något som däremot är möjligt är att sätta upp en tjänst för nyckeldistribution. Då behovet av nyckeldistribution har funnits länge finns det flera kända modeller för detta.

4.2.5 Intrångsskydd

Data kan föras in och ut ur ett datorsystem över flera kanaler. Det innebär att en dator och ibland även enskilda applikationer, måste kunna upptäcka att någon försöker få tillgång via en kanal. Ett typiskt intrångsskydd är en brandvägg vilken kan läsa av, analysera och ibland även reagera på den trafik som passerar igenom brandväggen. Det finns dock fler vägar in i en dator vilket gör att alla portar måste bevakas. Det är möjligt att koppla intrångsskyddet till en central loggningstjänst i syfte att få ta del av den insamlade kunskapen från intrångsförsök på andra IT-system samt en möjligt snabbare uppdatering av signaturer i händelse av ett angrepp. Utöver analys skulle en tjänst kunna administrera till exempel brandväggen.

4.2.6 Intrångsdetektering

Intrångsdetektering kan utföras på värddatorn (eng. host-based intrusion detection) eller på hela nätverket (eng. network-based intrusion detection). Intrångsdetekteringssystemet samlar in trafik och reagerar på förutbestämda eller ovanliga händelser. Säkerhetsloggarna som nämndes tidigare är ett exempel på information ett intrångsdetekteringssystem kan nyttja.

För att uppnå en bättre bild av vad som föregår i nätverket eller runt ett IT-system kan analyser från intrångsdetekteringssystemet vidarebefordras till ett centralt intrångsdetekteringssystem. På samma sätt som för säkerhetsloggning

blir det övergripande systemet lite trubbigare men ger samtidigt en bredare bild viken täcker in alla IT-system i nätverket.

4.2.7 Skydd mot skadlig kod

Skadlig kod kommer in i IT-system på samma sätt som övrig kod. Sannolikheten för att upptäcka den skadliga koden ökar om den kommer från det egna nätet i och med att koden då måste passera igenom fler skyddsfunktioner. Skadlig kod som kommer direkt in i ett IT-system, till exempel via ett USB-minne, måste kunna detekteras direkt på maskinen.

En säkerhetsfunktion för skydd mot skadlig kod består av en sensordel samt en analysdel. Sensor (det kan vara flera) lyssnar av trafik och skickar de vidare till en analysdel. Analysdelen undersöker innehållet i trafiken i syfte att identifiera kända mönster på skadlig kod. Insamlingen och analys ligger sannolikt lokalt för att kunna hantera alla möjliga kanaler in i ett IT-system. Det är dock möjligt att hantera säkerhetsfunktionen som en tjänst för trafik som kommer ifrån nätverket. Konfiguration och underhåll kan erbjudas som en tjänst.

5 Dynamiska tjänster

Säkerhetsfunktioner kan ofta upplevas statiska i sin funktion; antingen blir man inloggad eller inte, alternativt antingen får man åtkomst eller inte. Vad som styr beslutet att godkänna en inloggning eller åtkomst till ett dokument är idag statiskt och kopplat till individen. Om en behörig individ kan komma åt aktuellt system så antas förutsättningarna var uppfyllda för att ge åtkomst. En något mer nyanserad kontroll skulle kunna vara möjlig om en mer dynamisk modell för säkerhet skulle användas.

För att kunna avgränsa omfattningen och för att enklare ge exempel har ett beslut tagits inom projektet att fokusera arbetet mot åtkomstkontroll. Valet av åtkomstkontroll beror dels på funktionens mångsidighet men även den framtida roll en åtkomstkontrolltjänst antas ha i en objektbaserad säkerhetsmodell.

I nuläget är åtkomstkontroll i huvudsak inriktad mot sekretess. Åtkomstmodeller bygger på statiska accesskontrollistor eller någon form av rollbaserad åtkomstkontroll. Accesskontrollistor är bitvis omständliga att uppdatera, men framför allt tar det tid i ett större system. Ett system med statiska accesskontrollistor är således inte att föredra om förändringar sker ofta eller med kort förvarning. Rollbaserade system är något mer lätthanterliga då fokus för inloggning flyttas från individen till den roll individen innehar. Även rollbaserade system är dock statiska i sin natur (Debar et al., 2007).

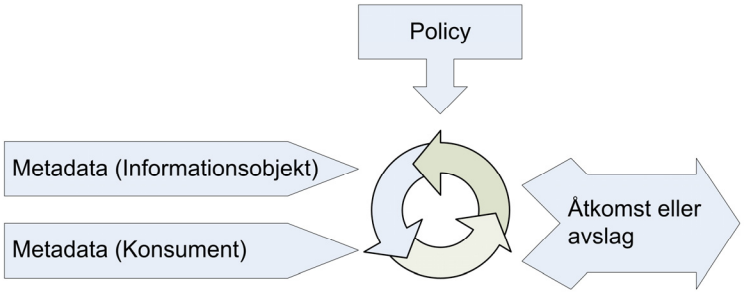
Vad är det då som gör en åtkomsttjänst dynamisk? Dynamisk har inom projektet identifierats som en policy vilken kan välja vilka regler som den ska följa beroende på vilka attribut som presenteras. I sin enklaste form skapas dynamik genom att ett antal förutbestämda handlingsalternativ fastställs. Växlingen mellan dessa alternativ sker sedan på en chefs order eller genom en privilegierad medarbetare. Att vara beroende av ett mänskligt beslut kan bromsa upp beslutsprocessen. För enklare beslut, till exempel för små och entydiga informationsobjekt, borde en automatiserad process vara rimlig.

Med en automatisk åtkomstprocess påverkas beslutet av fler egenskaper än enbart genom den frågandes identitet. Att ta med egenskaper såsom geografisk position kan åtkomst till ett dokument tillfälligt nekas eller medges beroende på vad positionsreferensen innebär för behovet och omgivningen.

5.1 Attributbaserad åtkomstkontroll

En åtkomstmodell som kan hantera flera egenskaper är attributbaserad åtkomstkontroll (eng. Attribute-Based Access Control). Ett attributbaserat åtkomstsystem hanterar tre informationsklasser; subjekt, resurs, samt miljö. Subjektklassen beskriver den användare som efterfrågar en resurs. Det viktigaste att få ut ur subjektklassen är användarens identitet. Egenskaper såsom roll,

arbetsplats, med mera, kan vara ett stöd för en mer dynamisk åtkomstkontroll, men samtidigt är detta uppgifter som oftast redan finns lagrade i, exempelvis, en användarkatalog. Resursklassen skulle kunna hanteras på samma sätt som subjektklassen, det vill säga att det är identiteten på resursen som är essentiellt. Så länge åtkomstkontroll är det enda som efterfrågas kan även resursens egenskaper kunna vara lagrade i ett centralt uppslagssystem. Om informationsobjektet dessutom skall vara sökbart via attributen måste de finnas på objektet. Miljöklassen är den mest föränderliga klassen i modellen. Miljön runt användaren kan variera mycket beroende på om användaren är på sin arbetsplats, på resande fot, på mission, et cetera. Det innebär att miljöklassen skulle kunna innehålla attribut som beskriver geografisk position, roll, tid, aktuellt nätverk, med mera. Attributen från respektive klass är indata till den policy som skall bedöma om åtkomst skall medges. Att en policy styr vilka attribut som är intressanta gör att modellen ibland även kallas policystyrd åtkomstkontroll. Figur 2 ger en översiktlig bild över ett attributbaserat åtkomstkontrollsystem.

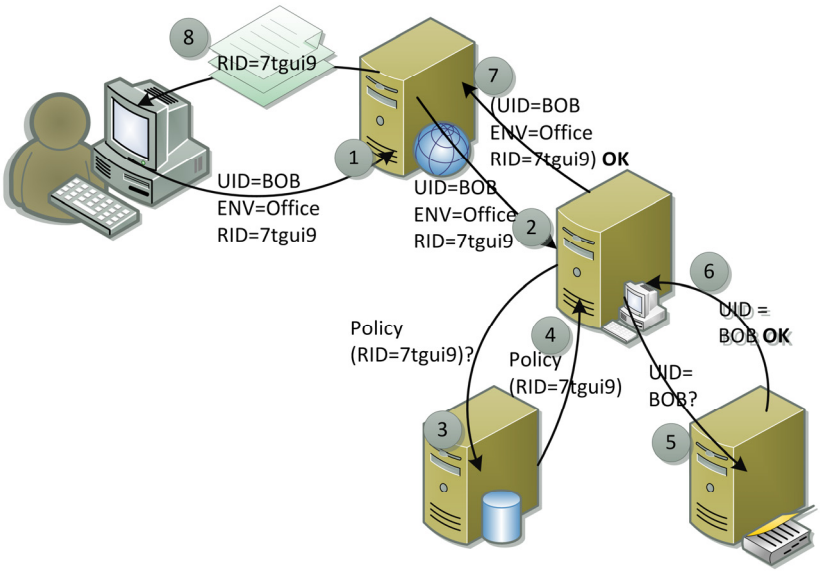


Figur 2: Attribut- och policystyrd åtkomstkontroll.

Möjligheten att välja attribut medför att policyreglerna kan se högst olika ut. I det enklaste fallet skulle till exempel räcka med användaridentitet för att medges åtkomst till det efterfrågade dokumentet. I ett annat fall skulle mer detaljerade krav vara möjliga inom samtliga informationsklasser. Figur 3 och 4 visar två möjliga scenarier där olika informationsmängder krävs för att få åtkomst.

I Figur 3 vill BOB få tillgång till en handling med resursidentiteten (RID) 7tgui9. Samtidigt som BOB skickar en förfrågan till resursservern följer en miljöbeskrivning (ENV) med förfrågan [1]. I det här fallet befinner sig BOB på sitt kontor (OFFICE). IT-systemet där den efterfrågade resursen finns vidarebefordrar BOBs förfrågan till en policyserver (2). Policyservern begär att få de policyregler som gäller för resursen 7tgui9 (3). Aktuella regler för 7tgui9 returneras till policyservern (4). Nu vet policyservern vilka attribut som är aktuella för det här beslutet. I och med att policyn den här gången endast krävde en behörig användare kan policyservern ignorera miljöklassen och enbart

verifiera BOB gentemot en katalogtjänst (5, 6). När BOB är verifierad är policyn uppfylld och policyservern returnerar ett OK till resursservern. Resursserven skickar begärd resurs till BOB.



Figur 3: Exempel 1 Attributbaserad åtkomstkontroll.

Figur 4 visar ett annat exempel där policyn innehåller några fler regler. Policyn kräver här att BOB skall vara på kontoret under normal tjänstgöringstid (07:00-18:00) samt att BOB måste tillhöra enheten G7.

REQUEST
Subjektklass
UID=BOB
Miljöklass
ENV=Office
TID=22:12:35
Resursklass
RID=7tgui9

POLICY
Resursklass
RID=7tgui9
Subjektklass
UID=*
Miljöklass
ENV=Office
TID=07:00:00-18:00:00
UNIT=G7

Figur 4: Exempel 2 Utökad policy.

Policyn i Figur 4 anger utöver ett tidsintervall även en tillhörighet som inte skickas med förfrågan. I och med att BOB kan verifieras (steg 5 i Figur 3) mot en användarkatalog, kan även uppgiften om organisatorisk hemvist hämtas där. I exemplet i Figur 4 begär BOB tillgång till resursen utanför det angivna tidsintervallet och blir därmed nekad åtkomst.

5.2 Metadatabeskrivningar

Den attributbaserade åtkomstkontrollen är naturligt beroende av att den metadata som utgör attributen är korrekt och konsistent. För att det skall vara möjligt att skriva policyregler med ett förutsägbart resultat kan inte mängden och variationen av metadata vara oändlig. En organisation måste definiera en egen standard eller välja att följa någon av de internationella initiativ som finns.

För att underlätta skapandet av policys är det dock lämpligt att utveckla stödsystem i syfte att få ett konsistent skrivsätt.

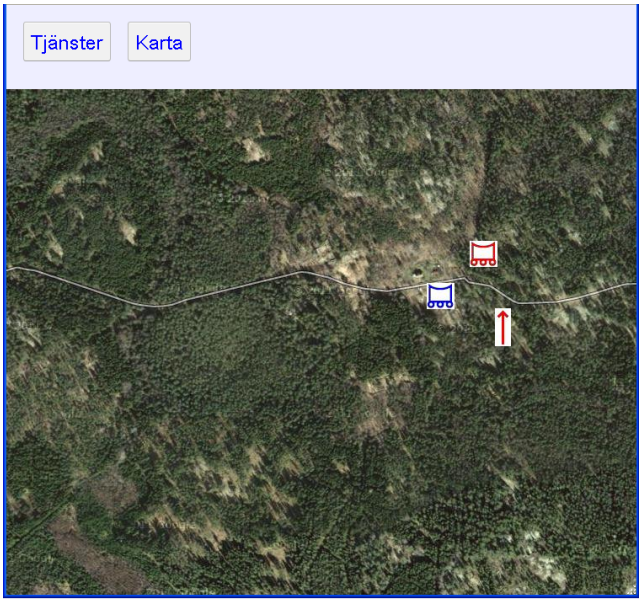
Sekretessbelagda handlingar skall i dagsläget märkas upp med aktuell informationssäkerhetsklass. Målsättningen, bland annat inom NATO, är dock att informationsobjekt endast skall beskriva vad de innehåller och att beslutet om sekretessgrad och därmed åtkomst tas av åtkomsttjänsten. Tanken bakom detta är att en sekretessbedömning gäller för stunden men utreds varje gång informationsobjektet efterfrågas. Med märkning följer idag även en hanteringsmodell vilken i stort bygger på fysisk separation. Det gör märkningen mer statisk då en användare eller ett system inte har möjlighet att efterfråga sekretessmärkta informationsobjekt.

5.3 Proof of Concept av attributbaserad åtkomstkontroll

Som avslutning av arbetet med attributbaserad åtkomstkontroll implementerades ett enklare system för gemensam lägesbild. Systemet visar på två typscenarier; (1) tillgång till tjänster beroenden på miljövariabler, samt (2) tillgång till information beroende på miljövariabler. Scenario (1) är ett inloggningsscenarie där säkerhetsklassning av konsumenten styr tillgången till tjänster. Scenario (2) är ett geografisktscenario där avståndet mellan en patrull och den plats informationen handlar om utgör beslutsgrund.

Figur 5 visar den gemensamma lägesbilden i scenario 2. En patrull (blå symbol i figuren) färdas längs vägen i östlig riktning (höger i figuren). Ett annat förband observerar fientlig verksamhet (röda symboler i figuren) på en plats som ligger i färdriktningen för patrullen. Då händelserna inte är kopplade till samma uppdrag är denna information inte allmänt tillgänglig för alla. Patrullen har dock behov av informationen i och med att innehållet av informationen, den observerade

fientliga verksamheten, kan få stor påverkan på patrullen och dess möjligheter att genomföra sin uppgift. I det här fallet skulle patrullen bli behörig till informationen enbart för att de befinner sig på eller i anslutning till den plats där informationen har ett värde. Med tillgång till informationen om den fientliga verksamheten kan patrullchefen förutse problem och fatta mer informerade beslut.



Figur 5: Scenario 2 - gemensam lägesbild.

Den regel som möjliggör för patrullchefen att se informationen är en zon runt en koordinat. Förbandet som observerade verksamheten har angett koordinaterna för verksamheten och policyregeln har satt en zon runt angivelsen, inom vilka egna förband får tillgång till informationen. Patrullen uppdaterar kontinuerligt sin position under framryckningen viket innebär att de kommer att hamna inom den aktuella zonen för den fientliga verksamheten, i och med att den ligger i färdriktningen. Om regeln med zonen tas bort kommer patrullen inte att veta något om den fientliga verksamheten innan de själva observerar den.

Indata till systemet kommer från användaren i form av användar- och miljöklasser med attribut, samt från resursen genom attribut i resursklassen. Policymotorn söker igenom de regler som finns och som har attribut som överensstämmer med de som angetts i de inkommande klasserna. Om en regel påträffas som stämmer med förutsättningarna beviljas tillgång till informationen. Ej uppfyllda regler eller avsaknad av regler medför att tillgång nekas.

6 Objektbaserad säkerhet

Projektet har haft till uppgift att följa utvecklingen inom området objektbaserad säkerhet (fråga IV i stycke 1.1). Det finns flera uppfattningar och målbilder med vad som är rimligt att uppnå med objektbaserad säkerhet. Ytterligheterna i diskussionen handlar å ena sida om krypterade informationsobjekt, vilket motsvarar krypterade filer, och hur tillgång till dekrypteringsnyckeln skall hanteras. Den andra sidan utgörs av ett informationsobjekt med inbyggda aktiva säkerhetsmekanismer som reglerar hur, var och när informationsobjektet får användas, vilket skulle innebära att informationsobjektet fungera som ett eget IT-system.

6.1 Kommersiella initiativ

Det kommersiella och akademiska intresset för området har varierat över tiden. Framförallt har dessa båda grupperingar olika målsättningar med objektbaserad säkerhet. Initialt var det kommersiella intresset främst styrt av frågor rörande digitala rättigheter (eng. Digital Rights Management, DRM) och hur dessa skulle kunna bevaras. Det var medieområdet med skiv- och filmbolag som gick i spetsen som ville skydda sina produkter. De fanns dock ett parallellt spår vilket syftade till att hantera styrning av rättigheter på filer för kontorsapplikationer, såsom textdokument. Gemensamt för båda inriktningarna var behovet av att utnyttja funktionalitet som finns i Microsoft Windows. Problemet med att vara tvingad till att använda funktioner i ett operativsystem är att producenten måste lita på att denna funktionalitet och att informationsobjekten är tvingade att använda densamma. En vanlig lösning är att producenten tillverkar egna hårdvarumoduler vilka måste användas för att få full funktionalitet. Detta är dock en dyr lösning, både för producent och för konsument.

Intresset för digitala rättighetslösningar har inte minskat med åren men mottagandet har varit svalt bland konsumenter. Däremot har intresset och utvecklingen gått vidare genom att försöka nyansera bilden av vad informationssäkerhet innebär. Det är framförallt IBM som fått uppmärksamhet med konceptet *Data-Centric Security* (Bilger et al., 2006). IBM:s modell syftar primärt till att trycka beslutsprocessen avseende åtkomstkontroll närmare informationsobjektets ägare samt att visa att detta är görbart med existerande teknologi.

6.2 Akademiska initiativ

En undersökning genomfördes för att se vilka akademiska initiativ som finns med en möjlig realisering inom fem till tio år. Undersökningen gav tre kandidater; distribuerad tvingande åtkomstkontroll (eng. Mandatory Access

Control, MAC), nät av informationsobjekt samt användningsstyrning (eng. Usage Control).

Tvingande åtkomstkontroll är en känd teknik för att hantera säkerhetsåtkomst inom ett operativsystem. En systemägare sätter åtkomstregler för alla informationsobjekt som hanteras inom IT-systemet. Underliggande system tvingas följa dessa regler. Genom att beskriva åtkomstregler i en policy och distribuera denna till IT-system som är tvingade att följa policyn. Metoden förutsätter att det mottagande operativsystemet kan förstå märkningen i huvudet på ett Internet Protokollpaket (IP-paket) eller att det finns en dedikerad virtuell maskin för ändamålet.

Nät av informationsnät (Jacobsen et al., 2009) är i första hand ett nytt sätt att se på information och dess spridning. Målet är att individuella informationsobjekt skall vara direkt sökbara och det inte skall ha någon betydelse varifrån informationsobjekten hämtas, så länge det är rätt informationsobjekt. Det viktigaste är att kunna fastställa identiteten på ett informationsobjekt. Målet med projektet är att flytta fokus få tillit från systemen som lagrar informationen till informationsobjektet själv.

Användarstyrning (Park & Sandhu, 2004) är den akademiska versionen av distribuerad rättighetskontroll. Inom området finns två huvudinriktningar; kryptgrafiskt skydd samt isolering av betrodda processer. Kryptografiskt skydd påminner mycket om den enklaste versionen av objektbaserad säkerhet som beskrevs i inledningen av det här kapitlet. Information skyddas med kryptering till dess att en licenstjänst verifierat mottagarens behörighet. Isolering av betrodda processer påminner om strukturen inom tjänstebaserad åtkomstkontroll med en vakt- och beslutspunkt (policyservern i Figur 3).

6.3 Kärnfrågeställningar

Den huvudsakliga målsättningen med objektbaserad säkerhet är tillgänglighet. Det innebär att ett informationsobjektets fysiska plats inte skall vara avgörande för dess tillförlitlighet. I och med att det inte finns en given plats att hämta informationsobjektet på måste informationsobjektet föra med sig mer information om var och hur säkerhetstjänster kan nås så att informationsobjektets integritet kan verifieras samt, om det är skyddat, hur åtkomst erhålls. Två centrala frågeställningar kan identifieras utifrån detta.

1. Hur märks information så att märkningen alltid följer informationsobjektet och inte kan ändras?
2. Hur hanteras tillgången till de nycklar som kommer att krävas för verifiering och dekryptering?

Informationsmärkning med metadata är dels ett tekniskt problem vad avser tilliten till att metadatan är korrekt och att den är läsbar för flera plattformar. Dels är ett informationsproblem. Metadatan skall guida konsumentens IT-system till att verifiera och dekryptera informationsobjektet samt stödja IT-systemen som möjliggör detta. Samtidigt får inte metadatabeskrivningarna, när sekretess är inblandat, avslöja innehållet i informationsobjektet.

Nyckelhantering är ett klassiskt problem inom kryptoområdet. Med objektbaserade lösningar kommer nyckelmängden sannolikt att öka och så även behovet av tillgång till nycklar.

7 Sammanfattning

Projektet *Objekt- och tjänstebaserad säkerhet* har pågått i tre år. När projektet startade var tjänsteorientering (eng. Service Oriented Architecture, SOA) ett etablerat begrepp men det gällde främst traditionella målsättningar med system som transformerats om till tjänster. Web services som teknik hade funnits några år och mognat. Dock hade tekniken inte fått det väntade genomslag som visionärerna förespråkat. Framför allt var det uppslagstjänsten Universal Description Discovery and Integration (UDDI) som inte accepterats på marknaden. Web services levde inom lokala nät men spridningen som en global resurs var inte efterfrågad på det sätt som tekniken presenterades. Efterföljande tekniker som Software-as-a-Service och numera molntjänster har hittat tillämpningar inom företag och organisationer.

Säkerhetsfunktionalitet har inte utvecklats i samma takt. Den ursprungliga säkerhetsmodellen med ett starkt perimeterskydd är fortfarande levande även om den är utsatt för hård kritik och modifieringar. Teknikutvecklingen med mobila plattformar har medfört, utöver tjänste- och molnorienteringen, att definitionen av in och utsida för en organisations nätverk försvåras. I militära sammanhang avlöser missioner varandra vilket innebär att samarbete med nya koalitionspartners upprättas och avslutas oftare och snabbare än förr. Behovet av flexibla IT-system som kan tillgodose tillgänglighet samt som är enkla att anpassa efter nya miljöer och samarbetspartners är stort.

Säkerhet handlar i grund och botten om kontroll, vilket står i ett motsatsförhållande till den efterfrågade tillgängligheten. Säkerhetslösningar som är implementerade på de system som de skall skydda kan vara svåra eller omständliga att hantera ur ett verksamhetsperspektiv. Lokala system medför en större mängd uppdateringspunkter och därmed en större osäkerhet över genomslag när systemöverskridande policyförändringar görs. Målet med att försöka skapa tjänsteorienterade säkerhetsfunktioner är, likt målet för tjänsteorientering i övrigt, att uppnå flexibla och tillgängliga system.

Inom projektet valdes åtkomstkontroll som guidande exempel för tjänsteorientering samt för att visa på hur mer dynamiska åtkomstmodeller kan skapas. Attributbaserad åtkomstkontroll har visat sig vara mycket lovande som flexibel teknik. Valet påverkades även av de krav som en framtida objektbaserad säkerhetsmodell bedöms ställa på åtkomstkontroll.

8 Framtida arbete

Behovet av en ny säkerhetsmodell med fokus på informationssäkerhet framför systemsäkerhet är påtagligt. Det finns idag flera olika typer av nätverk och målsättningen för flera forskningsgrupper är att få information att kunna överföras sömlöst mellan dessa. Det ställer krav på att information måste kunna röra sig friare men även på att information inte alltid kommer att vara tillgänglig från sin ursprungliga plats. Förmågan att verifiera korrektheten av informationen måste dock vara möjlig vilket talar för tjänstebaserade säkerhetslösningar och information som till högre andel än tidigare får ansvara för sitt eget skydd.

Märkning av informationsobjekt och tekniker för att säkerhetsställa att märkningen är korrekt och att innehållet efterlevs kommer att vara kritiskt för tilltron till de objektbaserade säkerhetssystemen. Attributbaserad åtkomstkontroll kommer sannolikt att spela en viktig roll i ett sådant system.

9 Referenser

Bilger, M., O'Connor, L., Schunter, M., Swimmer, M., Zunic, N., *Data-centric security*. IBM, december 2006.

Debar, H., Thomas, Y., Cuppens, F., Cuppens-Boulahia, N., "Enabling automated threat response through the use of a dynamic security policy". *Journal in Computer Virology*, volym 3 nummer 3, augusti 2007.

Department of Defense, *Department of Defense Net-Centric Data Strategy*, 30 april 2003.

Flygelholm, S., Norlander, A., Hansson, L-Å., *Expeditionär förmåga*. Försvarsmakten, 31 oktober 2008.

Försvarsmakten, *CIO Måldokument för Nät- och Informationsinfrastruktur (NII)*. HKV 09 100:64095, 24 september 2009.

Försvarsmakten, *Krav på säkerhetsfunktioner (KSF), version 2.1*. 10 750: 78976, 20 december 2004.

Hafner, M., Breu. R., *Security engineering for service-oriented architectures*. Springer, 2009.

IBM, *Using SOA to Transform People, Processes and Information*. IBM Cooperation, 2007.

Jacobson, V., Smetters, D.K., Thornton, J.D., Plass, M.F., Briggs, N.H., Braynard, R.L., "Networking Named Content". *CoNEXT'09*, Rom, Italien, 1-4 december 2009.

NATO Consultaion, Command and Control Agency, *NATO Network Enabled Capability Feasibility Study volume II: Detailed report covering a strategy and roadmap for realizing an NNEC networking and information infrastructure (NII), version 2.0*. Juni 2005.

NATO Consultaion, Command and Control Agency (NC3A), *NATO Network Enabled Capability Feasibility Study Volume 1: NATO Network-Centric Operational Needs and Implications for the Development of Net-Centric Solutions, version 2.0*. Oktober 2005.

Organization for the Advancement of Structured Information Standards, *OASIS Reference Model for Service Oriented Architecture 1.0*. OASIS Standard, 12 oktober 2006. http://docs.oasis-open.org/soa-rm/v1.0/ (2011-11-13).

Park, J., Sandhu, R., "The UCONABC Usage Control Model". *ACM Transactions on Information and System Security*, volym 7 nummer 1, februari 2004.

Peterson, G., “Service-Oriented Security Indications for Use”. *IEEE Security & Privacy*, volume 7 issue 2, mars-april 2009.

10 Projektpublikationer

10.1 2009

Bengtsson, A., Westerdahl, L., *Virtual Machines - Security Qualities*. FOI användarrapport, FOI-R--2904--SE, december, 2009.

Westerdahl, L., *Objekt- och tjänstebaserad säkerhet: Handlingsplan*. FOI Memo 2840, 7 juni 2009.

Westerdahl, L., *Problem Statement – Service and Object-based security*. FOI användarrapport, FOI-R--2825--SE, september, 2009.

10.2 2010

Bengtsson, A., *Objektbaserad säkerhet - En statusrapport*. FOI Memo 3386, 30 november 2010.

Karlzén, H., *Metadata för objekt- och tjänstebaserad säkerhet*. FOI användarrapport, FOI-R--2974--SE, mars, 2010.

Westerdahl, L., *Objekt- och tjänstebaserad säkerhet: Projektstatus*. FOI Memo 3208, 7 juni 2010.

Westerdahl, L., *Objekt- och tjänstebaserad säkerhet – Årsrapport*. FOI användarrapport, FOI-R--3093--SE, november, 2010.

Westerdahl, L., *Sammanfattning av IST-096-möte*. 8-11 november 2010. FOI Memo 3385, 30 november 2010.

10.3 2011

Karlzén, H., *Dynamisk policy för objekt och tjänstebaserad säkerhet*. FOI Memo 3547, 12 april 2011.

Westerdahl, L., *Objekt- och tjänstebaserad säkerhet – Projektstatus*. FOI Memo 3622, 16 juni 2011.

Westerdahl, L., *Sammanfattning av IST-096-möte, 18-21 april 2011*. FOI Memo 3556, 4 maj 2011.

Westerdahl, L., *Objekt- och tjänstebaserad säkerhet.* Användarrapport, FOI-R--3361--SE, december 2011.