Objektbaserad säkerhet

Årsrapport 2013

LARS WESTERDAHL

FOI-R--3802--SE
ISSN 1650-1942 December 2013

Lars Westerdahl

Objektbaserad säkerhet

Årsrapport 2013

Bild/Cover: Lars Westerdahl

Titel	Objektbaserad säkerhet - Årsrapport 2013
Title	Object-Based Security - Annual Report 2013
Rapportnr/Report no	FOI-R--3802--SE
Månad/Month	December
Utgivningsår/Year	2013
Antal sidor/Pages	26 p
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	E36049
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informations- och aerosystem

Sammanfattning

Den här rapporten sammanfattar de aktiviteter och de uppdrag som har genomförts inom FoT-projektet Objektbaserad säkerhet under 2013. Den huvudsakliga uppgiften för projektet har varit att studera möjligheten att realisera en IT-säkerhetsmodell där säkerhetsfunktionalitet knyts direkt till ett informationsobjekt och på så sätt minskar informationsobjektets beroende av ett systembaserat perimeterskydd. Inom frågeställningen ingår även att studera hur åtkomstkontroll kan förbättras genom en mer finmaskig kontrollfunktion. De tekniker som har varit i fokus för årets arbete är attributbaserad kryptering och attributbaserad åtkomstkontroll.

En del av arbetet sker genom ett samarbete med Natoforskningsgrupperna Information Assurance / Cyber Defence Research Framework och Trusted Information Sharing for Partnerships.

Nyckelord: Objektbaserad säkerhet, Obs, Attributbaserad kryptering, ABE, Attributbaserad åtkomstkontroll, ABAC, Obemannade farkoster, UAS, Cybersäkerhet

Summary

This report summarizes the activities and tasks that have been performed within the FoT-project Object-Based Security during the year of 2013. The main task for the project has been to study the possibilities to realize a security model where security functionality is tied directly to a data object, thus becoming less dependent of a system-oriented perimeter protection. Within the context of the project's main questions, there is also a task to study how access control can be refined by the use of a more fine-grained control function. The techniques that have been the focus of this year's research are Attribute-Based Encryption and Attribute-Based Access Control.

The project is partially performed as a collaboration with the NATO research groups Information Assurance / Cyber Defence Research Framework and Trusted Information Sharing for Partnerships.

Keywords: Object-Based Security, OBS, Attribute-Based Encryption, ABE, Attribute-Based Access Control, ABAC, Unmanned Autonomous Vehicles, UAS, Cyber security.

Innehåll

1 Inledning

Säkerhetsfunktioner[1] för informationstekniksystem (IT-system) har i första hand utvecklats för att skydda IT-systemen mot omvärlden. Efter hand som informationsteknologin utvecklats och mognat som användningsområde har det blivit allt svårare att separera vad som är insida av ett system från vad som är utsida. Numera är det inte bara människor som vill utbyta uppgifter mellan varandra, även IT-system är idag i stor utsträckning starkt integrerade med varandra. Fysisk separation, så kallade luftgap, är ett av de vanligaste sätten att skydda ett känsligt IT-system från omvärlden. Ett luftgap är dock inget garanterat skydd från utsidan även om det minskar den möjliga angreppsytan. Samtidigt som angreppsytan minskar, så minskar även den egna förmågan att kommunisera. I flertalet kommunikations- och ledningssystem är behovet av att utbyta information så stort att ett manuellt processande av uppgifter över ett luftgap är otillräckligt.

Skyddsmekanismer skall dock inte enbart skydda mot ofrivilligt informations-läckage. Det finns flera legitima anledningar till att låta uppgifter lämna en skyddad zon. I en samarbetssituation vill en informationsägare kunna dela uppgifter med mottagare på ett effektivt sätt. Det kan innebära att uppgifter kan behöva placeras på lagringsplatser vilka befinner sig utanför uppgiftsägarens kontroll eller där skalskyddet är okänt. Här behövs ett skydd som verkar direkt på informationsobjektet utan att vara beroende av omgivningens skyddskapacitet.

Alla säkerhetsproblem uppkommer dock inte enbart på utsidan av en skyddad zon. Om ett skalskydd utgör den enda skyddsmekanismen finns inget skydd för uppgifter i ett system om skalskyddet kan förbigås eller om en användare med åtkomst till systemet kan övertalas att till exempel stjäla uppgifter som ligger utanför dennes arbetsuppgifter.

Det finns ett behov av att kunna skydda uppgifter både från interna och externa hot, vare sig de är antagonistiska eller mer av nyfikenhetskaraktär.

Objektbaserad säkerhet är en idé om hur säkerhetsfunktionalitet kan knytas direkt till ett informationsobjekt och därmed göra upprätthållandet av säkerhets-egenskaperna mindre beroende av den omgivande funktionaliteten. På så sätt förväntas en högre spridningsgrad av uppgifter vara möjlig utan att för den skull ge avkall på övriga säkerhetskrav.

[1] Säkerhet kan åsyfta skydd mot kroppslig skada och olyckor (eng. safety) eller skydd mot ett medvetet angrepp (eng. security). I den här rapporten avser säkerhet innebörden i det engelska ordet security.

1.1 Mål med projektet

Projektet Objektbaserad säkerhet startade 2012 och kommer att avslutas 2014. Målbilden för projektet är att kunna påvisa ett lösningsförslag på hur objektbaserad säkerhet kan uppnås.

1.2 Nytta för Försvarsmakten

Försvarsmakten deltar idag i ett flertal koalitioner. Inom dessa finns behov av att dela uppgifter med andra men med olika önskemål om spridning av dessa uppgifter. Deltagare i en koalition kan dessutom ansluta eller lämna koalitionen under pågående uppdrag vilket gör att en mottagare av uppgifter inte alltid kan beskrivas som en viss individ, utan måste beskrivas med egenskaper vilka beskriver den roll som mottagaren representerar.

Utvecklingsarbetet inom Nato av Federating Mission Networking (FMN) stödjer de riktlinjer som anges i NATO Network Enabled Capability (NNEC). Det innebär bland annat att man inom Nato hellre vill ha federationer av system än ett dedikerat system som alla medlemmar och partners behöver anpassa sig till. Informationsdelning inom en sådan federation kräver nya policys för effektiv informationshantering (Grelier 2012). Utvecklingen av objektbaserad säkerhet stödjer detta tankessätt och bidrar till ett automatiserat och policyreglerat system.

1.3 Rapportens uppbyggnad

I kapitel 2 beskrivs de områden och aktiviteter som genomförts inom ramen för projektet under 2013. I kapitel 3 presenteras de internationella samarbeten som projektet deltagit i eller medfinansierat.

2 Genomförd verksamhet

Arbetet inom projektet Objektbaserad säkerhet sker huvudsakligen i två spår. Huvudfrågeställningen avseende hur förutsättningar för objektbaserad säkerhet skapas efterforskas i huvudsak inom projektgruppen. En komplementerande frågeställning om hur beslutet om åtkomst kan förbättras genomförs genom ett internationellt samarbete med Natogruppen Trusted Information Sharing for Partnerships.

Projektet deltar även i en bredare satsning, där även FOI:s övriga FoT-finansierade IT-säkerhetsprojekt ingår, genom att studera frågor rörande assurans och cyberförsvar. Detta arbete genomförs inom ramen för Natoprojektet Information Assurance / Cyber Defence Research Framework.

I det är kapitlet presenteras det arbete som utförts inom projektet Objektbaserad säkerhet under året, både internt och inom ramen för Natosamarbete. De båda Natogrupper som nämnts här presenteras närmare tillsammans med andra internationella samarbeten i kapitel 3.

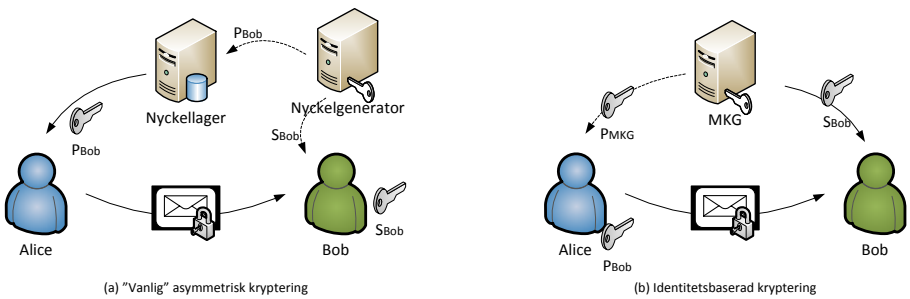
2.1 Egenskaper för objektbaserad säkerhet

Informationssäkerhet för elektroniska informationsobjekt har i huvudsak åstadkommits genom att skyddsfunktioner integrerats i de system där informationsobjekt är lagrade alternativt i direkt anslutning till systemet. Resultatet har blivit att informationsobjektet kan skyddas så länge de är lagrade eller endast används inom uppgiftsägarens säkerhetsdomän. När behov uppkommer av att dela information med andra parter utanför säkerhetsdomänen eller om en medarbetare tillfälligt arbetar utanför säkerhetsdomänen minskas därmed skyddsförmågan vilket kan öka riskerna relaterade till att uppgifter exponeras för obehöriga.

Objektbaserad säkerhet är en modell för informationsdelning där skydds-mekanismer kopplas direkt till ett informationsobjekt. Den direkta kopplingen mellan informationsobjekt och skyddsmekanism syftar till att möjliggöra att informationsobjektet skall kunna flyttas utanför informationsägarens säkerhets-domän utan att skyddet för informationsobjektet för den skull minskar. Just förmågan att bevara ett informationsobjekts sekretess och riktighet utanför en informationsägares säkerhetsdomän är en nyckelegenskap inom objektbaserad säkerhet. Andra betydande egenskaper är att kunna styra åtkomst till informationsobjektet utanför säkerhetsdomänen genom en policy. Den policyreglerade åtkomsten bör helst kunna ske autonomt, det vill säga utan att

konsumenten[2] behöver kontakta producentens[3] åtkomstkontrollsystem. Behovet av autonomitet kan variera, men det viktigaste är att en grundfunktionalitet skall kunna erbjudas utan garanterad åtkomst till ett givet stödsystem. Under 2013 har attributbaserad kryptering (eng. Attribute-Based Encryption, ABE) studerats som en möjlig kandidat för att tillgodose de grundläggande egenskaperna inom objektbaserad säkerhet.

Attributbaserad kryptering är ett relativt nytt område inom kryptering vilket introducerades av Amit Sahai and Brent Waters (2005) som en vidareutveckling av identitetsbaserad kryptering. När identitetsbaserad kryptering introducerades (Shamir 1985) vände den på modellen för hur asymmetriskt krypterad kommunikation upprättas. De dittills använda krypteringsmodellerna förutsatte att mottagaren i förväg skapat och publicerat en publik nyckel och att avsändaren hade tillgång till denna. Figur 1a beskriver ett förenklat förlopp för att skicka ett krypterat meddelande. Bob vill få sina mejl i krypterad form för att säkerhetsställa en privat kommunikation. Bob begär en hemlig nyckel, *SBob*, och en publik nyckel, *PBob*, från en *nyckelgenerator*. Den publika nyckeln skickas till ett *nyckellager* så att den kan nås av alla som vill kommunicera med Bob, medan Bob själv sparar sin hemliga nyckel. Alice vill skicka ett meddelande till Bob och hämtar Bobs publika nyckel från nyckellagret. Med Bobs publika nyckel, *PBob*, kan Alice kryptera ett meddelande och skicka till Bob. När Bob tar emot det krypterade meddelandet kan han dekryptera meddelandet med sin privata nyckel, *SBob*.



Figur 1: Asymmetrisk kryptering.

Shamirs (1985) modell med identitetsbaserad kryptering kräver inga i förväg distribuerade nycklar mellan sändare och mottagare. Figur 1b beskriver en

[2] En konsument är en mottagare av informationsobjekt. Det kan vara den slutliga mottagaren och den som nyttjar uppgiften i informationsobjektet men det kan även vara en mellanhand.
[3] En producent tillhandahåller informationsobjekt antingen som skapare, ägare eller som mellanhand.

generaliserad bild av identitetsbaserad kryptering. Centralt för identitetsbaserad kryptering är en *Master Key Generator, MKG*. Alice vill skicka ett meddelande till Bob. De har aldrig kommunicerat krypterat förut och har således inte utbytt krypteringsnycklar tidigare. Första gången Alice vill kommunicera krypterat med någon måste hon begära MKG:s publika nyckel, P_{MKG}. Med MKG:s publika nyckel kan Alice skapa krypteringsnycklar för alla som är knutna till samma MKG. I fallet med Bob kombinerar Alice MKG:s publika nyckel och en för Bob unik identitet, till exempel hans mejladress. Alice har nu skapat Bobs publika nyckel, P_{Bob}, och kan skicka ett meddelande krypterat till Bob. När Bob tar emot meddelandet måste han begära sin hemliga nyckel, S_{Bob}, från MKG för att kunna dekryptera meddelandet. Nu kan Alice skicka meddelande till Bob och Bob kan läsa dessa utan inblandning av MKG:n så länge nycklarna giltiga.

Attributbaserad kryptering bygger vidare på samma modell som identitetsbaserad kryptering genom att generalisera modellen samt lägga till en policy. I identitetsbaserad kryptering finns en identitet vilket gör att kommunikationen endast riktas till en mottagare. Kommunikationen är även förutsättningslös, det vill säga att så länge mottagaren kan styrka sin identitet gentemot MKG:n så erhåller mottagaren sin privata nyckel. För att kunna hantera flera urvalskriterier än en given identitet introducerades attribut som godtyckliga indata till den publika nyckeln. Till dessa attribut kopplades en policy för hur attributen skulle utvärderas. På så sätt generaliseras mottagaren till att representera allt från en unik person till en grupp eller en specifik förutsättning.

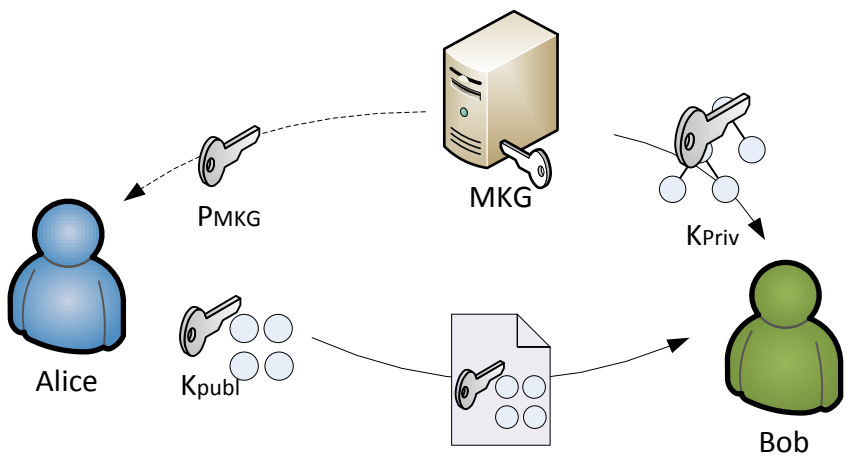
När Sahai och Waters (2005) skapade attributbaserad kryptering var det primära målet att förbättra metoden för identitetsbaserad kryptering av biometrisk data vid autentisering. Biometriska avläsningar av fingeravtryck, iris, med mera innehåller oftast små avvikelser beroende på små förändringar i exempelvis mätpunkter eller olika sensorer. För att hantera detta krävs en viss tolerans vid jämförelse av lagrad biometrisk data och den avläsning som görs vid en autentisering. Detta innebar att deras initiala policy var av typen *k av x*, det vill säga att *k* attribut av *x* möjliga skall överensstämma. Ganska snart utvecklades dock mer användbara och uttrycksfulla policys vilka antingen kopplas till mottagaren eller till den fil som skall krypteras. Dessa metoder kallas för Key-Policy Attribute-Based Encryption respektive Ciphertext-Policy Attribute-Based Encryption och beskrivs närmre i kommande avsnitt.

2.1.1 Key-Policy Attribute-Based Encryption

Key-Policy Attritbute-Based Encryption (KP-ABE) (Goyal, Pandey, Sahai & Waters 2006) var den första versionen av attributbaserad kryptering med en uttrycksfull policy. I KP-ABE tillskrivs en fil med ett antal attribut vilka kommer att ligga till grund för den policy som mottagaren av filen skall utvärderas emot. Policyn kan beskrivas som ett träd där de nedersta noderna (löven) utgör attribut och alla överliggande noder motsvarar, i den enklaste versionen, de logiska

grindarna AND och OR. En policy som exempelvis avgränsar behöriga läsare till ekonomisektionen eller juridiksektionen på högkvarteret kan skrivas som ”ekonomi” AND ”hkv” OR ”juridik” AND ”hkv”. En mottagare av en fil med dessa attribut och som har en policy som uppfylls kan därmed dekryptera filen. Saknas attributet ”hkv” eller sektionen visar på något annat än ”ekonomi” eller ”juridik” kan inte policyn uppfyllas vilket resulterar i att filen förblir krypterad.

Figur 2 visar översiktligt processen för KP-ABE. Alice vill kryptera en fil för att sedan göra den tillgänglig för en del inom sin organisation. Precis som i identitetsbaserad kryptering måste Alice hämta MKG:s publika nyckel, *PMKG*, första gången som hon skall utföra en kryptering. Alice väljer ut den fil hon vill dela och skapar en krypteringsnyckel, *Kpubl*, baserad på MKG:s publika nyckel och ett antal attribut som beskriver målgruppen. Filen krypteras med *Kpubl* och görs tillgänglig, exempelvis via e-post eller en gemensam lagringsplats. Bob, som arbetar inom samma organisation och med liknande uppgifter som Alice, har en dekrypteringsnyckel, *Kpriv*, innehållande en policy som anger Bobs tillhörighet och vilka dokumenttyper Bob får åtkomst till. Överensstämmer attributen i filens krypteringsnyckel och Bobs dekrypteringsnyckel samt att policyn i dekrypteringsnyckeln uppfylls kan Bob läsa filen.



Figur 2: Key-Policy Attribute-Based Encryption.

Två möjliga tillämpningsområden för KP-ABE som föreslogs av Goyal et al. (2006) var undersökning av loggfiler samt reglering av broadcastsändningar. En typisk loggfil innehåller mycket information och åtkomst till loggfilen innebär vanligtvis åtkomst till hela innehållet. Med KP-ABE kan åtkomst regleras för administratören baserat på de attribut som loggfilen innehåller. På så sätt kan man dela upp ansvaret mellan administratör och därmed undvika att hela

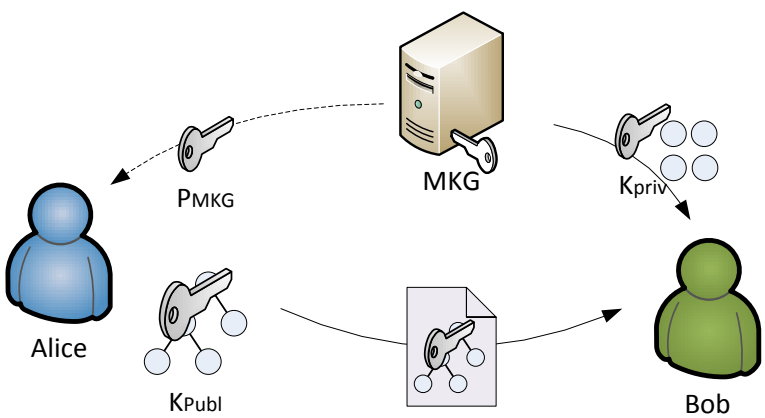
behörigheten till loggfilen hamnar på en administratör. Två administratörer kan heller inte samverka för att få en utökad åtkomst tack vare att KP-ABE är designat för att undvika den typen av försökt till ökade privilegier.

Den andra tillämpningen rör broadcastsändningar. Informationsägaren, i det här fallet en medialeverantör, märker olika program med attribut såsom namn, säsong och avsnitt medan mottagaren har en policy som anger vilka program i utbudet som denne har åtkomst till baserat på aktuell prenumeration. På så sätt kan informationsägaren skicka ut ett flöde och låta filtrering ske hos mottagaren istället för att skicka flera olika flöden.

Tekniken för hantering av broadcastsändningar borde även gå att anpassa för Försvarsmaktens behov. En möjlig tillämpning skulle vara inom konceptet gemensam lägesbild. Om inkommande informationsobjekt krypteras och associeras med attribut som beskriver dess tänkta mottagare enligt tekniken för KP-ABE kan en policy associeras en mottagare genom dennes dekrypterings-nyckel. På så sätt skulle samma informationsflöde kunna gå till flera mottagare i krypterat format, men mottagaren har endast möjlighet att se den del som motsvarar mottagarens behörighet.

2.1.2 Ciphertext-Policy Attribute-Based Encryption

Ett i de flesta fall mer naturligt sätt att använda attributbaserad kryptering kallas för Ciphertext-Policy Attribute-Based Encryption (CP-ABE) (Bethencourt, Sahai & Waters 2007). Metoden är också mer lik de ursprungliga tankarna från Sahai & Waters (2005).



Figur 3: Cipher-Policy Attribute-Based Encryption

Alice (se Figur 3) har erhållit MKG:s publika nyckel, *PMKG*, och vill nu kryptera en fil. Alice väljer en fil och fastställer en policy för en uppsättning attribut och skapar en publik nyckel, *KPubl*. Policyn beskriver relationen mellan de attribut som utgör urvalfaktorer. Alice krypterar filen med *KPubl* och kan därefter publicera filen på en publik lagringsyta. Bob, som tillhör samma MKG som Alice, autentiserar sig mot MKG:n och erhåller en dekrypteringsnyckel, *Kpriv*. Bobs dekrypteringsnyckel utgörs, förutom av MKG:s publika nyckel, av en uppsättning attribut vilka beskriver Bob. Det innebär att Bob inte behöver hämta en ny nyckel när nya krypterade meddelanden kommer även om de är krypterade med olika policys. Så länge Bobs attribut stämmer med policyn kan Bob dekryptera filen.

Molntjänster är ett av de huvudsakliga tillämpningsområdena för attributbaserad kryptering. Ett problem med molntjänster är att de oftast ligger utanför en informationsägares säkerhetsdomän vilket ofta gör informationsägaren tveksam till att göra informationsobjekt tillgängliga på sådana platser. Med möjligheten att koppla både ett skydd (kryptering) och en åtkomstkontroll (policy) till en fil öppnas möjligheter för att kunna använda mindre betrodda lagringsplatser. CP-ABE har flera tillämpningsområden inom molntjänster. Müller (2011) utvecklar bland annat Luo, Hu & Chens (2010) idéer om att tillämpa CP-ABE inom serviceorienterad arkitektur (eng. Service Oriented Architecture, SOA). Även om SOA inte är skapat med en objektbaserad säkerhetsmodell i åtanke visade det sig dock möjligt att åstadkomma detta utan att förändra protokollen i alltför stor utsträckning.

2.1.3 Tillämpning av attributbaserad kryptering inom objektbaserad säkerhet

Möjligheten att med attributbaserad kryptering kryptera ett meddelande och att kunna koppla en policy till ett informationsobjekt, ger en möjlighet att uppfylla objektbaserad säkerhets grundkrav på att kunna flytta ett informationsobjekt utanför informationsägarens säkerhetsdomän. En mer komplex tillämpningsmiljö kan vara Federated Mission Networking (FMN). FMN är Natos framtida metod för att koppla samman fasta ledningsstrukturer och missionsnät under en mission. Resurserna under en mission är naturligt rörliga eftersom de tillhandahålls av deltagarna vilka kan ansluta och lämna missionen allteftersom. Deltagarna i en mission utgörs av Nato, Natos medlemsländer och icke-Natoländer i partnerroller (North Atlantic Treaty Organization (Nato) 2012). I en sådan kontext kan en mer informationsorienterad säkerhetslösning möjliggöra informationsdelning även om förutsättningarna och medlemmarna varierar.

Attributbaserad kryptering är dock fortarande ett ungt forskningsområde, vilket gör att det ännu löpande sker betydande förbättringar inom området samt att det inte finns några kommersiella tillämpningar som utnyttjar tekniken. Som forskningsområde är det dock mycket intressant för objektbaserad säkerhet.

Avsaknaden av tillämpningar gör att de problem som diskuterats inom litteraturen avseende attributbaserad kryptering i huvudsak fokuserar på teoretiska problem. Mer administrativa problem som uppkommer vid realisering av lösningar såsom möjlighet att använda gruppolicys och fördefinierade attribut är ännu utanför fokus för den forskning och utveckling som bedrivs inom området.

2.2 Förfinad åtkomstkontroll

Funktioner för åtkomstkontroll innebär oftast en begränsad möjlighet att fatta ett åtkomstbeslut som är anpassat för aktuella förutsättningar. Oftast är åtkomst-kontrollen baserad på identiteten på den som frågar efter en resurs eller möjligtvis dennes roll i sammanhanget. Dessa förutsättningar är dock konstanta vilket innebär att identitet och, om så är fallet, roll alltid ger samma resultat vid en förfrågan oavsett när frågan ställs eller varifrån den ställs. Genom att föra in fler variabler i beslutsprocessen kan ett åtkomstbeslut även baseras på upp-fattningen om det aktuella säkerhetsläget. Tillämpningar av attributbaserad åtkomst finns bland annat i form av attributbaserad kryptering vilken beskrevs ovan i avsnitt 2.1 och som attributbaserad åtkomstkontroll (eng. Attribute-Based Access Control, ABAC) (Hu, Ferraiolo, Kuhn, Schnitzer, Sandlin, Miller & Scarfone 2013). Målet för dessa metoder är att fatta ett åtkomstbeslut baserat på de attribut som presenteras av den som efterfrågar en resurs, resursens attribut och kontexten där frågan ställs. För att förstå hur en policy behöver utformas så att den motsvarar den skyddsnivå som informationsägaren önskar, behöver en förståelse för vilka attribut som utgör urvalsgrund upparbetas.

Säkerhetsegenskaper för informationssäkerhet beskrivs oftast utifrån egenskaperna sekretess (eng. confidentiality), riktighet (eng. integrity) och tillgänglighet (eng. availability). Allt som oftast tillkommer ytterligare egenskaper, exempelvis oavvislighet (eng. non-repudiation), ansvarighet (eng. accountability), auktorisation (eng. authorization), autentisering (eng. authentication) (SIS 2007), innehav eller kontroll (eng. possession or control), äkthet (eng. authenticity) samt användbarhet (eng. utility) (Parker 2010).

Sekretess har, i alla fall för militär verksamhet, en relativ entydig tolkning för de högre informationssäkerhetsklasserna (HEMLIG/SECRET och högre). Även om betydelsen av informationssäkerhetsklassen mer omfattar konsekvens av ett röjande av uppgiften i fråga, finns det ett regelverk kopplat till informations-säkerhetsklasserna vilka anger hur uppgifter skall hanteras. Motsvarande tolkning finns föreslagen för riktighet och tillgänglighet (MSB 2009), men har inte uppnått samma acceptans. Det är vanligare att riktighet och tillgänglighet har flera tolkningar beroende på i vilken situation de tillämpas.

Frågor rörande riktighet och tillgänglighet som urvalkriterier för åtkomstbeslut studeras i samarbete med Natoforskningsgruppen Trusted Information Sharing for Partnerships (Tisp), Inom ramen för Tisp diskuteras för närvarande för- och nackdelar med en riktighets- respektive en tillgänglighetsmärkning av typen som (SIS 2006) föreslår eller om det är bättre att identifiera ett antal attribut som genom en policy kan bedöma aktuellt behov av riktighet och tillgänglighet enligt modellen för attributbaserad åtkomstkontroll (Hu et al. 2013).

Den uppenbara fördelen med en specifik riktighets- respektive tillgänglighets-märkning är att det inte råder något tvivel om vad som avsågs vid märknings-tillfället. Å andra sidan så är det svårt vid märkningstillfället att veta hur framtiden och dess behov ser ut. När det gäller sekretess är en märkning alltid tillfällig, det vill säga att den anger vilket utslag en bedömning fick senast. En ny bedömning skall dock alltid göras när en sekretessbelagd handling efterfrågas. Det samma borde gälla för en riktighets- respektive tillgänglighetsmärkning.

Informationsobjekt märkta med beskrivande attribut och en policy som konsulteras varje gång ett informationsobjekt efterfrågas ger förutsättningar för beslut fattade baserat på den aktuella situationen. Ett attributbaserat åtkomst-system ställer dock stora krav på informationsägaren och de stödjande IT-systemen. De attribut som associeras till ett visst informationsobjekt måste beskriva innehållet i informationsobjektet på ett uniformt sätt utan att för den delen röja innehållet, i alla fall inte om det rör sig om ett informationsobjekt innehållande uppgifter belagda med sekretess. Den policy som ligger till grund för åtkomstbeslutet måste hållas uppdaterad för att systemet skall kunna fatta åtkomstbeslut på aktuella grunder.

Oavsett om informationsobjekt märks med en bedömning av behovet eller genom en uppsättning attribut sker bedömningen baserat på en policy. Skillnaden ligger främst i om den mesta tilltron till bedömningen tillfaller människan eller en maskin. En användare kan göra en bedömning i samband med att informations-objektet skapas och märka objektet. De grunder som användaren gör sin bedömning på är inte nödvändigvis väl strukturerade utan mer en magkänsla eller rutin. Tilltron till maskinell bedömning är svår att värdera men ger en högre effektivitet, något som är viktigt för system med en hög grad av trafik.

Tillämpningen av en förfinad åtkomstkontroll kan föras tillbaka till attribut-baserad kryptering för att ge bättre och tydligare policys. Den teknik som sannolikt vinner mest på detta är traditionell åtkomstkontroll utökad med en attributbaserad bedömningsfunktion. Användandet av flera attribut kommer att ge en kostnad för validering av policy i form av längre beräkningstider. I fallet attributbaserad kryptering växer dessutom längden på nyckeln, och därmed även informationsobjektet, i takt med antalet attribut. Därmed inte sagt att attribut-baserad kryptering är en olämplig lösning för skydd av informationsobjekt, men det verkar än så länge vara effektivare med en traditionell åtkomstmodell så länge kommunikation med stödsystem inte är begränsad. Inom Tisp diskuteras

flera aktuella tillämpningsområden där en mer finmaskig åtkomstmodell tros göra nytta. Ett exempel på sådana tillämpningsområden är Cyber Defence Data Collaboration and Exchange Infrastructure (CDXI) vilket är ett automatiserat informationsdelningssystem för uppgifter förande cyberförsvar (Fernández Vázquez, D., Pastor Acosta, O., Spirito, C., Brown, S. & Reid, E. 2012). Federated Mission Networking (FMN) nämndes tidigare i samband med tillämpningar av attributbaserad kryptering. Inom FMN finns i nuläget en bedömningsfunktion kallad Clearinghouse vilken är en manuell funktion för att bedöma vilken information som kan släppas utanför en säkerhetszon. Målsättningen inom FMN är att kunna automatisera den här processen så fort tillit till en sådan funktion kan erhållas (Grelier 2012).

NATO Communication & Information Agency tillämpar attributbaserad åtkomstkontroll i ett automatiserat system de har utvecklat (NATO Communication & Information Agency (NCIA) 2013a). Systemet gör skillnad på policy för att skydda uppgifter, det vill säga regler för hur uppgifter skall hanteras internt, och vad som gäller för spridning av uppgifter, vilket mer motsvarar traditionell åtkomstkontroll. Systemet befinner sig ännu på demonstratornivå.

Deltagande vid möten inom Tisp finns dokumenterade i två FOI Memo (Westerdahl 2013c; Westerdahl 2013d).

2.3 Cyberförsvar

En uppgift för projektet är att aktivt följa arbetet inom Natoprojektet Information Assurance (IA) / Cyber Defence (CD) Research Framework. De arbetsuppgifter som FOI genomför därinom har i år främst inneburit att ta fram en problemställning avseende cyberhot mot marina autonoma system samt att göra en uppdatering av de tidigare framtagna scenarierna för kollaborativ utveckling av cyberförsvarsfunktionalitet.

En av de deltagande organisationerna inom IA / CD Research Framework är Centre for Marine Research & Experimentation (CMRE). CMRE forskar bland annat på obemannade undervattensfarkoster och olika tillämpningar för dessa. Inom CMRE:s arbete har främst robust undervattenskommunikation varit i fokus, vilket har medfört att de än så länge inte studerat cybersäkerhetsaspekter i exempelvis ubåtsjaktsscenarier. För att stödja CMRE och för att testa IA / CD Research Frameworks framtagna forskningsramverk utför FOI ett arbete med att beskriva cybersäkerhetsmiljön i ett framtida sensorbaserat ubåtsjaktsscenario samt i ett hamnövervakningsscenario. Resultatet av detta arbete kommer att publiceras i IA / CD Research Frameworks slutrapport, vilken färdigställs under våren nästa år.

IA /CD Research Framework har också till uppgift att beskriva en prototypmiljö där två parter kan samarbeta vid prototyputveckling av skyddsmekanismer för att möta cyberhot. Prototypmiljön är i sig själv än så länge bara en modell, men för att utvärdera modellens möjligheter har gruppen i ett tidigare arbete tagit fram ett flertal scenarier där modellen används. FOI:s uppgift består i att välja ut scenariobeskrivningar som beskriver modellens funktionalitet väl och som gör den tydlig. IA / CD Research Frameworks rapport som beskriver prototypmiljön kommer att slutföras under våren nästa år.

Deltagande på möten inom IA / CD Research Framework finns dokumenterade i två FOI Memo (Westerdahl 2013a; Westerdahl 2013b).

2.4 FoT seminariedag

Objektbaserad säkerhet deltog i den årliga seminariedag som organiseras av FOI:s tre FoT-finansierade IT-säkerhetsprojekten. Årets upplaga genomfördes på Tre Vapen i Stockholm tisdagen den 29 oktober med cirka 25 deltagare från Förvarsmakten, Försvarets materielverk och Försvarshögskolan.

Programmet bestod av en inledande resultatpresentation där projektet Objektbaserad säkerhet tillsammans med projekten Effektivare hot-, risk- och sårbarhetsanalyser samt Pålitliga IT-plattformar presenterade erhållna resultat från forskningsarbetet sedan föregående års seminariedag. Därefter vidtog projektvisa diskussioner.

Inom området objektbaserad säkerhet presenterades arbetet med attributbaserad kryptering. De frågeställningar som uppkom under presentationen rörde i huvudsak säkerheten runt nyckelgenerering och hantering av nycklar hos mottagaren. Under diskussionsdelen framkom idéer om möjliga behov och exempel på tillämpning av en mer informationsorienterad skyddsfunktion jämfört med de mer vanliga systemorienterade skyddsfunktionerna. Ett informations-orienterat skydd skyddar inte enbart mot en yttre angripare, det har även möjlighet att skydda mot en intern angripare med åtkomst till systemet.

Seminariedagen avslutades med en gemensam debatt mellan projektmedlemmar och publik avseende Försvarsmaktens IT-säkerhetsbehov på fem till tio års sikt, skillnader i behov baserat på miljö samt vad cybermiljön innebär för Försvarsmakten. Huvuddelen av diskussionen rörde sig runt hur uppgifter hanteras i ytterkanten, ”nära fronten”. Här uppkom en diskussion om behovet av att hantera uppgifter som har behov av sekretess under en kort tidsperiod. Vilket systemstöd krävs för att hantera en sådan situation?

En sammanfattning från seminaridagen finns dokumenterad i FOI Memo ”Seminariedag 2013” (Bengtsson 2013).

3 Internationell samverkan

I det här kapitlet presenteras de internationella grupper som projektet Objektbaserad säkerhet samarbetar med direkt eller indirekt. Själva arbetet som FOI utför inom grupperna beskrivs i kapitel 2.

Det här året har utmärkts av en högre grad av internationella kontakter än vad som är vanligt. Projektmedlemmar har sedan tidigare varit aktiva inom Nato-forskningsgrupper och projektet har även medfinansierat ett EU-projekt. Nytt för i år är ett uppstartsarbete för ett bilateralt samarbete med USA genom Air Force Research Lab.

3.1 Samarbete med USA

Sverige har tillsammans med USA fört diskussioner de senaste två åren om att upprätta ett forskningssamarbete inom området cybersäkerhet. Området i sig är brett och har flera intressenter. I det här fallet har uppgiften ålagts FOI med stöd av Försvarsmakten och Försvarets materielverk. På amerikansk sida hanteras frågan av Air Force Research Lab (AFRL).

Under våren genomfördes en workshop i syfte att identifiera gemensamma intresseområden inom cybersäkerhet. Mötet varade i två dagar under perioden 24-25 april och genomfördes hos AFRL i Rome, New York. FOI deltog med tre personer och dess deltagande finansierades av IT-säkerhetsprojekten inom FoT.

Tabell 1: Presentationer under FOI-AFRL-möte.

FOI:s presentationer	AFRL:s presentationer
• ”Cyber Defence Exercise”	• ”ACE Hackfest”
• ”Operation analysis and experimentation in conjunction with cyber security exercises”	• (Ingen formell presentation gavs men ämnet diskuterades.)
• ”Cyber Risk Management”	• ”Mission assurance” • ”Survive and Recover”
• ” Security Culture and User Behavior”	• “National Operational Environment Model (NOEM)”
• ”Secure information sharing in coalitions”	• “Cross-Domain Information Sharing”
• ”Trusted Platforms”	• ”Trusted Systems”

Från FOI:s sida föreslogs sex samarbetsområden för vilka AFRL presenterade motsvarande arbete från sin sida (Tabell 1).

Inom ramen för ”Secure information sharing in coalitions” och ”Cross-Domain Information Sharing” diskuterades i första hand frågor rörande datamärkning och hur detta stödjer en datasluss (eng. Cross-Domain Solution). Här fanns även ett intresse för arbetet inom Natogruppen Trusted Information Sharing for Partnerships.

I de avslutande diskussionerna enades båda parter om att intressanta områden att samarbeta om främst är cyberförsvarsövningar, men även riskhantering i cybermiljö och säker informationsdelning i koalitioner.

Under tiden för det efterföljande nationella förankringsarbetet framkom även ytterligare ett önskemål om att samarbeta om cyberhot rörande autonoma obemannade farkoster (eng. Autonomous Unmanned Vehicles, AUV).

Det har ännu inte tagits något beslut om ett samarbete skall inledas och i vilken omfattning det i så fall skulle vara aktuellt.

3.2 Information Assurance / Cyber Defence Research Framework

Projektet Objektbaserad säkerhet finansierar tillsammans med de övriga FoT-projekten Effektivare hot-, risk- och sårbarhetsanalyser samt Pålitliga IT-plattformar deltagande i Natoforskningsgruppen Information Assurance (IA) / Cyber Defence (CD) Research Framework (se avsnitt 2.3 för en beskrivning av de arbetsuppgifter som FOI utfört inom gruppen i år). Arbetet inom IA / CD Research Framework har pågått sedan 2010 men befinner sig nu i sitt slutskede och kommer att avslutas under första kvartalet 2014.

IA / CD Research Framework syftar till att ta fram ett ramverk för hur forskning inom cyberförsvar kan organiseras och sättas i relation till övrig produktutveckling inom Nato. Som ett led i att beskriva cyberförmågor har gruppen fungerat som referensgrupp för NATO Communication and Information Agencys arbete med att ta fram en bred förmågebeskrivning för cyberförsvar (NCIA 2013b).

En annan del av IA / CD Research Frameworks arbete är att beskriva en prototypmiljö för kollaborativ framtagning av cyberförsvarsförmågor. Miljön möjliggör exempelvis för en part att skapa en målmiljö medan en annan part kan utveckla en specifik funktion.

Begreppet Cyber har fått mycket uppmärksamhet de senaste åren. Även om Försvarsmakten hittills inte har en uttalad cyberförmåga, finns ändå motsvarande

förmåga men under andra namn. Genom deltagande i IA / CD Research Framework ges insikt i hur andra nationer tänker och prioriterar inom området.

3.3 Trusted Information Sharing for Partnerships

Trusted Information Sharing for Partnerships (Tisp) är ett Natoforskningsprojekt vilket FoT-projektet Objektbaserad säkerhet är en del av. Tisp syftar dels till att ta fram en design för en Information Exchange Gateway (IEG), dels att studera hur egenskaperna riktighet och tillgänglighet kan förbättra ett åtkomstbeslut. (Se avsnitt 2.2 för en beskrivning av det arbete som FOI utför inom gruppen i år.)

Det scenario som IEG:n skall kunna hantera är informationsutbyte mellan ett skyddat Natonät och ett nät tillhörande ett icke-Natoland, internationella organisationer eller icke-statliga organisationer. De egenskaper som är gemensamma för dessa mottagare är att det inte med säkerhet går att uttrycka deras skyddsnivå avseende informationshantering på ett sådant sätt som en militär organisation är van vid, vare sig det rör sig om IT-system eller interna processer. Jämfört med tidigare scenarier där IEG endast exponerats mot, om än med lägre skyddsklass, andra Natonät, kommer IEG:n här att exponeras mot den allmänna sidan av Internet. Inom ramen för denna frågeställning har även frågor rörande pålitliga plattformar uppkommit, men det är inte en del av huvudfrågeställningarna. Tisp avser ta fram en design över en IEG som kan hantera detta scenario.

Intresset av att studera riktighet och tillgänglighet som utökade variabler för en mer finmaskig åtkomstkontroll har vuxit sig stark inom gruppen. Det har ännu inte framkommit en digital representation av denna märkning som fått en allmän spridning, även om förslag har tagits fram. Ett förslag kommer ifrån en tidigare Natoforskningsgrupp; XML in Cross Domain Security Solutions (Nato 2006). Det har inte producerats någon officiell slutrapport från den här gruppen men resultatet finns bland annat återgivet i (Haakseth 2012). Det finns inget givet mål inom Tisp att skapa en ny märkning för riktighet och tillgänglighet, utan målet är att diskutera möjligheterna att använda egenskaperna riktighet och tillgänglighet för att beskriva regler för åtkomst.

Metoder för åtkomstkontroll är kritiska för att uppgifter inte skall hamna i orätta händer. Ett för strikt hållningssätt kan dock leda till en ineffektiv organisation där interna aktörer och processer de facto motverkar varandra och därmed organisationens förmåga att utföra sin uppgift. Studier av verksamhetsmässigt effektivare åtkomstmetoder gynnar Försvarsmaktens förmåga att uppnå en effektiv informationsdelning inom sin egen organisation och med koalitionspartners.

Inom Tisp finns även en stark koppling mot utvecklingen av Federating Mission Networking (FMN). FMN är en viktig komponent för framtida koalitioner vilket gör den intressant för Nato, men även för Försvarsmakten som framtida koalitionspartner. Inom FMN är målsättningen att på sikt kunna införa en mer förfinad åtkomstkontroll, till exempel genom att värdera egenskaper (attribut) kopplade till en uppgift genom en policy.

Tisp startade 2012 och förväntas pågå till och med 2014.

3.4 FIDELITY

Projektet Objektbaserad säkerhet är med och delfinansierar FOI:s deltagande i EU-projektet ”Fast and trustworthy Identity Delivery and check with ePassports leveraging Traveler privacy (FIDELITY)” (Totalförsvarets forskningsinstitut u.å.). FIDELITY är en del av Europakommissionens sjunde ramprogram (European Commission u.å.) och som sådant finansieras FOI:s deltagande till 75 % av EU.

FIDELITY-projektets uppgift är att analysera brister och sårbarheter i livscykeln för elektroniska pass i syfte att rekommendera förbättringar och utveckla lösningar. Projektet presenterar lösningar för att förbättra processen för att upprätta ett pass, förbättra säkerheten i elektroniska pass och passens utökade användbarhet, stärka rutiner kring försvunna och stulna pass samt säkerställa individens integritet. FOI bidrar till arbetet inom områdena

- behovs- och protokollanalys,
- vidareutveckling av certifikathantering,
- systemtilltrohöjande åtgärder,
- bättre och effektivare metoder för verifiering av identitet.

Arbetet inom FIDELITY har främst gett utökade kunskaper inom områdena formulering och hantering av säkerhetskrav samt certifikatsdistribution och certifikathantering.

Säkerhetsarbetet inom FIDELITY utgår ifrån en hotanalys. I processen att omsätta hotanalysen till krav på säkerhetsfunktioner har flera erfarenheter dragits avseende hur dessa bör formuleras så att ett tydligt krav ställs. I samband med detta arbete har även förslag på lösningar framkommit.

Elektroniska pass är något som är avsett att användas i en internationell kontext. Själva passen har utöver de visuella uppgifterna även ett chip av typen Radio Frequency Identification (RFID), där de visuella uppgifterna är duplicerad samt ytterligare biometriska uppgifter tillagda. För att identifiera förfalskningar måste uppgifterna på RFID-chipet verifieras. Detta sker med stöd av digitala certifikat.

Tekniken för detta är beprövad men hur den tillämpas varierar från nation till nation.

När det gäller certifikathantering deltar FOI framför allt med att studera standarder för certifikathantering samt att genomföra en hot- och sårbarhetsanalys för den tänkta arkitekturen. Vid behov vidareutvecklas även protokoll för certifikathantering.

Certifikathantering mellan nationer är inte enbart ett tekniskt problem. Det är till exempel inte ovanligt att nationer vill vara huvudsaklig verifieringsinstans (eng. certification authority, CA) för sina medborgares uppgifter.

Erfarenheter från detta arbete ökar förmågan att förstå de behov som kan uppkomma när säkerhetsfunktioner behöver samarbeta eller kommunicera i exempelvis en koalition.

FOI deltar i FIDELITY-projektet till och med 2014. FIDELITY-projektet som helhet avslutas 2015.

Referenser

Bengtsson, J. (2013). *Seminariedag 2013* (FOI Memo 4656). Linköping: Totalförsvarets forskningsinstitut.

Bethencourt, J., Sahai, A. & Waters, B. (2007) Ciphertext-Policy Attribute-Based Encryption. I *SP '07, IEEE Symposium on Security and Privacy*, Berkeley, USA, 20-23 maj 2007, ss. 321-334. DOI: 10.1109/SP.2007.11

European Commission (u.å.). *Seventh Framework Programme (FP7)*. http://cordis.europa.eu/fp7/home_en.html [2013-12-03]

Fernández Vázquez, D., Pastor Acosta, O., Spirito, C., Brown, S. & Reid, E. (2012). Conceptual Framework for Cyber Defense Information Sharing within Trust Relationships. I CYCON 2012, Proceedings of the 4th International Conference on Cyber Conflict, 5-8 juni, Tallinn, Estland, ss. 429-445.

Grelier, P. (2012). *NATO Network Enabled Capability Federating the Future Mission Network*. https://www.act.nato.int/article-2012-2-19 [2013-12-02]

Goyal, V., Pandey, O., Sahai, A. & Waters, B. (2006). Attribute-based encryption for fine-grained access control of encrypted data. I *CCS '06, Proceedings of the 13th ACM conference on Computer and communications security*, Alexandria, USA, 30 oktober-3 november 2006, ss. 89-98. DOI: 10.1145/1180405.1180418

Hu, V.C., Ferraiolo, D., Kuhn, R., Schnitzer, A., Sandlin, K., Miller, R. & Scarfone, K. (2013). Guide to Attribute Based Access Control (ABAC) Definition and Considerations (draft)(NIST SP 800-162). Gaithersburg: National Institute of Standards and Technology.

Haakseth, R. (2012). *SOA Pilot 2011 – demonstrating secure exchange of information between security domains* (FFI-rapport 2012/00117). Kjeller: Forsvarets forskningsinstitutt.

Luo, S, Hu, J. & Chen, Z. (2011). Implementing Attribute-Based Encryption in Web Services. I *IEEE ICWS 2010, Proceedings of the 8th International Conference on Web Services*, Miami, USA, 5-10 juli, 2010, ss. 658-659. DOI:10.1109/ICWS.2010.82

Myndigheten för samhällsskydd och beredskap (MSB) (2009). *Modell för klassificering av information – Rekommendationer*. Karlstad: MSB.

Müller, S. (2011). *Data-Centric Security with Attribute-Based Encryption*. Diss. TU Darmstadt, Tyskland. Darmstadt: Univ.

North Atlantic Treaty Organization (Nato) (2006). *XML in Cross Domain Security Solutions (IST-068)*. http://www.cso.nato.int/Activity_Meta.asp?Act=1339 [2013-12-03]

North Atlantic Treaty Organization (Nato) (2012). *NATO Future Mission Network (FMN) Concept*, version 2. Norfolk, HQ SACT.

NATO Communication & Information Agency (NCIA) (2013a). *Content-based information Protection and Release in NATO operations*. Bryssel: NATO Communication & Information Agency.

NATO Communication & Information Agency (NCIA) (2013b). *Communication and Information System Security Capability Breakdown, Revision 4B* (Technical Report 2012/SPW008416/03). Haag: NATO Communication & Information Agency. [Förhandsutgåva, ej publicerad]

Parker, D. (2010). Our Excessively Simplistic Information Security Model and How to Fix It. *ISSA Journal*, juni, ss. 12-21.

Sahai, A. & Waters, B. (2005). Fuzzy Identity-Based Encryption Cryptology. I *EUROCRYPT 2005*, *Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Aarhus, Danmark, 22-26 maj 2005, ss. 457-473. DOI: 10.1007/11426639_27

Shamir, A. (1985). Identity-Based Cryptosystems and Signature Schemes. I *Advances in Cryptology, Proceedings of CRYPTO '84*, Santa Barbara, USA, 19-22 augusti 1984, ss.47-53. DOI: 10.1007/3-540-39568-7_5

Swedish Standards Institute (SIS) (2007). *SIS Handbok 550. Terminologi för informationssäkerhet*, utgåva 3. Stockholm: SIS Förlag AB.

Totalförsvarets forskningsinstitut (FOI) (u.å.). FIDELITY. http://foi.se/fidelity [2013-12-03]

Westerdahl, L. (2013a). *IST-096 Information Assurance / Cyber Defence Research Framework - åttonde mötet* (FOI Memo 4470). Linköping: Totalförsvarets forskningsinstitut.

Westerdahl, L. (2013b). *IST-096 Information Assurance / Cyber Defence Research Framework - nionde mötet* (FOI Memo 4677). Linköping: Totalförsvarets forskningsinstitut.

Westerdahl, L. (2013c). *IST-114 Trusted Information Sharing for Partnerships - femte mötet* (FOI Memo 4468). Linköping: Totalförsvarets forskningsinstitut.

Westerdahl, L. (2013d). *IST-114 Trusted Information Sharing for Partnerships - sjätte mötet* (FOI Memo 4675). Linköping: Totalförsvarets forskningsinstitut.

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