Objektbaserad säkerhet

Sammanfattning av projektet

LARS WESTERDAH, AMUND GUDMUNDSON HUNSTAD,
FREDRIK MÖRNESTEDT

FOI-R--4011--SE
ISSN 1650-1942 December 2014

Lars Westerdahl, Amund Gudmundson Hunstad,
Fredrik Mörnestedt

Objektbaserad säkerhet

Sammanfattning av projektet

Bild/Cover: (Fredrik Mörnestedt, FOI)

Titel	Objektbaserad säkerhet: Sammanfattning av projektet
Title	Object-Based Security: Summary of the Project
Rapportnr/Report no	FOI-R--4011--SE
Månad/Month	December
Utgivningsår/Year	2014
Antal sidor/Pages	36
ISSN	1650-1942
Kund/Customer	Försvarsmakten/Swedish Armed Forces
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	E36059
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Informations- och aerosystem

Sammanfattning

Denna rapport ger en sammanfattning av arbetet inom FoT-projektet Objekt-baserad säkerhet, vilket pågick mellan 2012 och 2014. Syftet med projektet var att undersöka vilka möjligheter det fanns att realisera en säkerhetsmodell där en säkerhetspolicy följer och verkar på ett informationsobjekt även efter att det har lämnat informationsägarens tekniska domän.

Arbetet har genomförts med två inriktningar. I första inriktningen studerades föreslagna lösningar inom forskningen, vilka kunde utgöra kandidater för en objektbaserad säkerhetsmodell. Särskilt studerades attributbaserad kryptering (eng. Attribute-Based Encryption, ABE) som visade sig ha goda förutsättningar att uppfylla målen genom att en säkerhetspolicy följer informationsobjektet vart än det flyttas. Med en säker uppkoppling mot informationsägarens system är ABAC (eng. Attribute-Based Access Control) som är en variant av attributbaserad åtkomstkontroll, en mognare och effektivare lösning.

Förmågan att beskriva användare, omgivning och informationsobjekt i mer detalj och att därmed skapa en policy som ger en mer dynamisk åtkomst, var projektets andra inriktning. Särskilt studerades vilka möjligheter som fanns att fokusera på riktighet (eng. integrity) och tillgänglighet (eng. availability) som grund för åtkomstbeslut.

Nyckelord: Attributbaserad åtkomstkontroll, attributbaserad kryptering, åtkomstkontroll, åtkomstkontrollpolicy.

Summary

This report summarises the work that has been performed within the FoT-project Object-Based Security, which lasted between 2012 and 2014. The purpose of the project was to investigate the possibilities of realizing a security model in which a security policy follows and governs an information object during and after it has left the information owner's technical domain.

The work has been carried out in two tracks. In the first track, proposed solutions within the research community were explored in order to find candidates which could fulfil the goals of an Object-Based Security model. Attribute-Based Encryption (ABE) in particular was explored, as it proved to have great potential to fulfil the goals. In an ABE solution, the security policy follows the information object, thus providing offline security. If a reliable connection to the information owner can be guaranteed however, Attribute-Based Access Control (ABAC) is a more mature and effective solution.

The ability to describe subjects, the environment, and information objects in more detail, thus creating a policy with more dynamic access rules was the project's second track. Although the effort was generic, integrity and availability properties were studied in more detail, to see how these properties could support an access decision.

Keywords: Attribute-Based Access Control, Attribute-Based Encryption, Access Control, Access Control Policy

Innehållsförteckning

1 Inledning

Objektbaserad säkerhet (Obs) är ett forskningsprojekt inom ramen för Forskning och teknikutveckling (FoT). Projektet har pågått under perioden 2012 till och med 2014. Den här rapporten syftar till att sammafatta de resultat som erhållits så här långt.

På informationssäkerhetsområdet finns ofta ett behov av en hög grad av automatik. Den mängd meddelanden som dagligen passerar till och från ett informationssystem i exempelvis en militär koalition är alltför omfattande för att en manuell beslutsprocess för delgivande av information till en mottagare skall vara effektiv.

För att en automatiserad kontrollfunktion ska kunna besluta om ett informationsobjekt kan skickas vidare till tänkt mottagare, eller om förfrågan skall nekas, måste enskilda informationsobjekt beskrivas på ett systematiskt sätt som underlättar sådan automatisering. Hittills har sekretess varit den viktigaste egenskapen vid åtkomstbeslut. Sekretess och de övriga egenskaperna i IT-säkerhetstriaden[1] – riktighet och tillgänglighet – används ofta för att beskriva hur ett IT-system skyddar den information som lagras. Resultatet har blivit att skydd av information i huvudsak handlar om vilka system som skyddar informationen när den är lagrad, när den exekveras och när den transporteras. Det är dock värt att notera att det inte är informationen i sig som är skyddad, utan informationsskyddet är en effekt av det skyddande systemet. Det innebär att informationen endast är skyddad så länge den finns inom de system som lyder under en säkerhetsdomän, det vill säga de IT-system som lyder och verkar under en gemensam säkerhetspolicy.

Den vanligaste arkitekturen i lokala nätverk och över internet är klient – server-modellen. Den innebär att en användare via sin klient (dator) frågar en server efter ett informationsobjekt. Om användaren är behörig till informationsobjektet skickar servern informationsobjektet till användaren. I samband med att informationsobjektet lämnar informationsägaren (avsändaren) – eller i bästa fall när informationsobjektet når mottagaren – förlorar informationsägaren all kontroll över informationsobjektet och det är upp till mottagarens godtycke att bevara skyddet av informationsobjektet.

Projektet Objektbaserad säkerhet syftar till att stödja Försvarsmaktens informationshantering genom att undersöka möjligheterna att låta informationsobjekt själva bära med sig det skydd som är nödvändigt för att bevara deras sekretess- och riktighetsbehov och samtidigt göra informationen mer tillgänglig.

[1] Sekretess (ibland konfidentialitet), riktighet och tillgänglighet. Från engelskans confidentiality, integrity och availability.

1.1 Frågeställningar

Målsättningen med projektet är att visa hur säkerhetsegenskaper kan följa med ett informationsobjekt när det lämnar informationsägarens system och hur dessa egenskaper kan bevaras över tiden.

För att uppnå detta har två huvudsakliga frågeställningar identifierats.

1. Hur binds säkerhetsbeskrivande data till informationsobjektet?
2. Hur säkerställs att informationsobjektets säkerhetsegenskaper bevaras hos mottagaren?

1.2 Genomförande

Arbetet inom projektet har genomförts i två inriktningar; teknisk lösning för objektbaserad säkerhet samt attributvärden för finmaskig åtkomstkontroll.

Inom inriktningen teknisk lösning för objektbaserad säkerhet har existerande tekniker för innehållsbaserad säkerhet (eng. Content-Based Security) analyserats med syftet att uppnå en säkerhetslösning med stor tillgänglighet av information. Målet var att identifiera en konceptuell lösning och en demonstrator för att påvisa möjligheten i en lösning för objektbaserad säkerhet.

Inom det andra spåret studerades vilka attribut som kan bidra till en uttrycksfull policy samt vilka värden dessa attribut kan anta, i syfte att ge en mer finmaskig åtkomstkontroll. Traditionellt har sekretess varit dominant säkerhetsegenskap, men i detta spår studeras hur även riktighet och tillgänglighet samt andra ytterligare egenskaper kan påverka åtkomstbeslut anpassat till den aktuella situationen. Arbetet med attributvärden har i huvudsak genomförts i samarbete med Natoforskningsgruppen IST-114 Trusted Information Sharing for Partnerships.

1.3 Läshänvisning

Rapportstrukturen följer utvecklingen från problem till lösning och avslutas med angränsande verksamhet som skett inom projektet samt slutsatser.

Kapitel 2 beskriver problembakgrunden samt presenterar visionen om objektbaserad säkerhet.

Kapitel 3 ger en överblick över de tekniska lösningar som potentiellt kan bidra till objektbaserad säkerhet.

Kapitel 4 beskriver arbetet med att identifiera attribut som beskriver de säkerhetsegenskaper som behövs för att åstadkomma åtkomstkontroll.

Kapitel 5 ger en överblick över samarbets- och kompetenshöjande aktiviteter som medlemmar ur projektet deltagit i, samt kunskapsförmedling.

Kapitel 6 sammanfattar de föregående kapitlen samt presenterar slutsatser.

2 Bakgrund

Detta kapitel redogör kortfattat för vilken potential som system baserade på objektbaserad säkerhet bedöms ha och hur de kan passa in i Försvarsmakten.

2.1 Visionen om Objektbaserad säkerhet

Samverkan och koalitionsarbete blir alltmer vanligt, vilket medför att det växer fram ett tydligt behov av att kunna utbyta och hantera information på ett säkert sätt utanför – och ibland utan kontakt med – den egna skyddande zonen. Objektbaserad säkerhet (Obs) innebär att säkerhetsfunktionalitet knyts direkt till informationsobjektet, för att möjliggöra att det bär med sig nödvändigt skydd utanför nuvarande informationssystem istället för att vara beroende av en skyddande zon. För att nå denna vision finns ett behov av att uppnå följande mål:

- Finmaskig policy för dynamisk informationsåtkomst och informationshantering.
- Säker tredjepartslagring av information utanför den egna zonen.
- Upprätthållande av åtkomstkontroll även i offlineläge.

Denna vision skulle innebära att information i större grad kan spridas mera öppet och även utanför en organisations eller verksamhets normala skyddande zon, utan att göra avkall på säkerheten.

2.2 Redan de gamla sumererna

Att säkerställa att riktig information når fram vid korrekt tid och i korrekt form är inte något nyligen uppkommet behov, utan har funnits långt bakåt i tiden. Vid utgrävningar kring floderna Eufrat och Tigris, samt i andra delar av Mellan-östern, har arkeologer hittat rikligt med små lerpolletter i utgrävningslager så långt tillbaka som år 8500 f.Kr. (Schmandt-Besserat 1982; Pettersson 1991; Robinson 1996; Alvegård 1994) Polletterna har givits en tydlig, nästan standardiserad utformning och haft teckenliknande markeringar. Trots detta, har polletterna tyvärr ofta bedömts vara ointressant skräp och inte tagits tillvara i någon större utsträckning. Senare forskning har dock bedömt att märkena och polletterna använts för bokföring. Olika polletter kan ha symboliserat olika varor eller ägodelar, men även kvantiteter av dessa. Från epoken 3500-3000 f.Kr. har lerbollar med lerpolletter inuti hittats. Lerbollarna har varit stämplade som en certifierande försegling av pollettinnehållet.

Lerbollarna anses ha använts som bokföringsdokument eller verifikation. Att bryta lerbollen och räkna antalet av olika polletter, möjliggjorde en kontroll. En herde som kom tillbaka till djurägaren med färre djur än han åkte iväg med, kan

då tänkas fått ett redovisningsmässigt problem. Lerbollarna och dess polletter kunde på samma sätt användas vid varutransporter som verifikation av förväntad leverans.

Ur perspektivet attributbaserad åtkomstkontroll kan det noteras att polletterna och bollarna utgjorde ett tidigt sätt att associera attribut som får, getter och sädesslag med värden som antal och volymer. Det var med andra ord ett sätt att tillhandahålla information till en förväntad mottagare (djurägaren, handlaren) vid en senare tidpunkt, eventuellt på ett annat ställe och i oförvanskad form (lerbollen har ej förstörts). Strikt taget är det dock inte tal om krypterad information, om det inte tas i beaktning att sannolikt endast ett fåtal torde ha haft förmågan att läsa informationen.

2.3 Hur passar Obs in i Försvarsmakten?

Under 2012 genomfördes en intervjubaserad studie för att inventera de informationssäkerhetsbehov som existerar i Försvarsmakten (Hunstad, Gustafsson, Karlzén, Mörnestedt & Westerdahl 2012).

Försvarsmakten är en stor organisation med många typer av verksamhet, från högre ledningsnivå till operativt militärt arbete men även dagligt myndighetsutövande. Denna variationsrikedom implicerar olika avvägningar, prioriteringar och behov avseende informationssäkerhet, en behovsbild som varierar i olika delar av Försvarsmakten.

Studien ledde fram till följande slutsatser:

Försvarsmakten har behov av ökad flexibilitet och tillgänglighet

Det finns ett stort behov av att samverka med andra aktörer inom och utanför koalitioner. Samarbetenas form och innehåll varierar mycket beroende på omständigheterna, vilket gör behoven svåra att förutse. Vidare är autonomitet ett viktigt behov inom Försvarsmakten.

Behovet av sekretess varierar inom Försvarsmakten

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

Försvarsmakten har behov av att hantera kontorssystem

Försvarsmakten är inte enbart en insatsorganisation utan även en myndighet. Det innebär att vardagen för många anställda innehåller interaktion med kontorssystem, till exempel för tidsrapportering och resebeställningar, men även för

utvecklingsarbete samt kontakt med externa parter. Det gör att Försvarsmakten i flera avseenden har samma behov av informationssäkerhet som andra myndigheter eller företag.

Obs är tekniskt möjligt att åstadkomma med dagens teknik

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

Målsättningen med Obs är att ge ökad tillgänglighet av information med bibehållen sekretess, spårbarhet och riktighet. Ur ett Försvarsmaktsperspektiv åstadkoms detta genom att Obs tillförs följande förmågor:

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

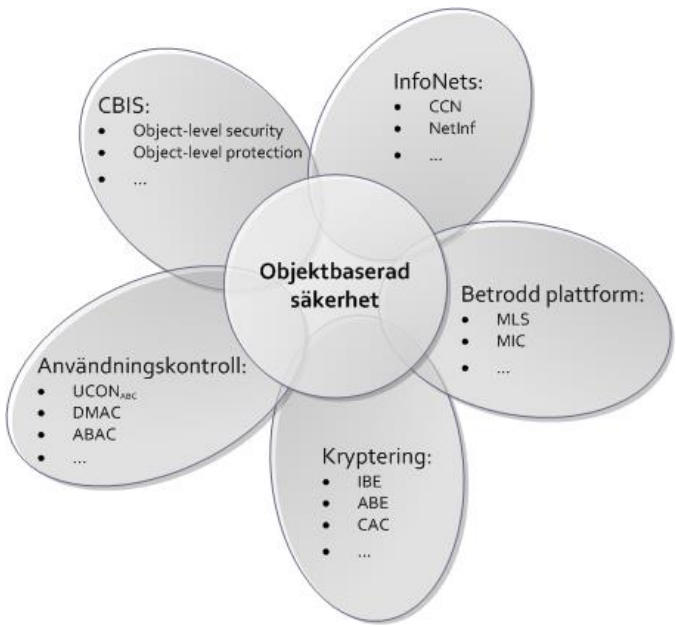
Förmågan spårbarhet har inte följts upp i arbetet med attributbaserad kryptering då detta inte stöds av metoden.

3 Lösningsrymd

Detta kapitel presenterar kortfattat utbudet av tänkbara tekniska lösningar för att utifrån Försvarsmaktens behov realisera Obs. En inom projektet framtagen demonstrator, som realiserar en del av Obs, beskrivs också.

3.1 Lösningsalternativ

Under projektets första år, 2012, genomfördes en litteraturstudie av forskning med inriktning som anknyter till visionen om Obs (Hunstad et al. 2012).



Figur 1 Forskningsområden relaterade till Obs (Hunstad et al. 2012).

Figur 1 illustrerar en uppsättning identifierade forskningsområden som på olika sätt relaterar till, och är intressanta att jämföra med, utvecklingen, intentionerna och potentialen rörande Obs. Med detta som utgångspunkt var tanken att identifiera vilka tekniker som var lovande kandidater för att uppfylla visionen om Obs.

Forskningsområdet användningskontroll utgör en generalisering av klassisk åtkomstkontroll. Generaliseringen innebär att autentisering och auktorisering sker kontinuerligt, inte endast vid öppnandet av ett informationsobjekt.

Utgångspunkten är med andra ord att all hantering av ett informationsobjekt utsätts för återkommande kontroll med avseende på vem som använder objektet, hur det används samt hur det transporteras och lagras. Inom forskningsområdet användningskontroll har Attribute Based Access Control (ABAC) bedömts som särskilt intressant ur Obs-perspektiv och diskuteras i avsnitt 3.2.

Forskningsområdet betrodd plattform utgörs av satsningar på att säkra informationshanteringen inom enskilda system. Informationsfokuserade nätverk (InfoNets) är ett forskningsområde där fokus istället är på nätverk och deras informationshantering medan Content Based Information Security (CBIS) berör informationshantering mellan säkerhetsdomäner.

Inom forskningsområdet kryptering bedömdes attributbaserad kryptering (eng. Attribute-Based Encryption, ABE) vara av särskilt intresse för närmare utvärdering och granskning varför det diskuteras vidare i avsnitt 3.2.

3.2 Attributbaserad åtkomstkontroll

Åtkomstkontroll har traditionellt tagit sin utgångspunkt i användaridentitet och knutit åtkomsträttigheter för informationsobjekt till denna. Attributbaserad åtkomstkontroll tar däremot sin utgångspunkt i egenskaper som beskriver användare, informationsobjekt och miljön där dessa verkar. Dessa egenskaper tillskrivs sedan användare, informationsobjekt och miljön genom attribut som enskilt eller i grupp kan tolkas av en policy när ett informationsobjekt efterfrågas. Exempel på attribut som kan användas är:

- Användare: namn, identitet, roll, formella behörigheter, mm.
- Informationsobjekt: titel, format, ägare, kategori, mm.
- Miljö: IP-adress, nätverksadress, geografisk position, tid, mm.

En policy kan användas av det kontrollerande systemet för att avgöra om rätt attribut är tillgängliga samt om relationen mellan attributen stämmer med policyn. Det kontrollerande systemet brukar i litteraturen oftast omnämnas som beslutspunkt eller Policy Enforcement Point (PEP). Attributbaserad åtkomst-kontroll illustreras av Figur 2.

En variant av attributbaserad åtkomstkontroll är ABAC. ABAC bygger på en klient – servermodell, vilket innebär att den kräver åtkomst till serverresurser för att realisera åtkomstkontroll. Systemberoendet möjliggör tillgång till aktuella uppgifter (attribut) om användare och informationsobjekt, samt ett större system-stöd för miljöattribut. Med avseende på Obs-visionens behov av att kunna hantera offlinesituationer, har ABAC dock fått en mindre roll inom projektet för tillfället.

Figur 2 Attributbaserad åtkomstkontroll

En annan variant av attributbaserad åtkomstkontroll är ABE som är centrerad kring en krypteringsmetod där policyn, beroende på ABE-variant, kan kopplas till ett krypterat meddelande eller till en mottagares dekrypteringsnyckel. I den mest omskrivna varianten av ABE krypterar informationsägaren ett informationsobjekt samt kopplar en policy till detsamma. Informationsägaren kan nu skicka informationsobjektet till önskad mottagare eller publicera det på en tillgänglig lagringsplats. En mottagare har erhållit en dekrypteringsnyckel som också innehåller en uppsättning attribut vilka beskriver mottagaren. Policyn i informationsobjektet medför att endast de mottagare som uppfyller policyn baserat på sina attribut kan dekryptera informationsobjektet. Genom att nyttja en policy istället för en given identitet som i PKI (Public Key Infrastructure) skapas en gruppnyckel vilket innebär att ett informationsobjekt kan delas till flera mottagare. En mottagare kan med sin attributförsedda dekrypteringsnyckel dekryptera godtyckliga meddelanden så länge de attribut som finns i informationsobjektets policy matchas samt att policyn uppfylls. Gruppegenskapen i ABE gör det möjligt att skapa en skyddad kommunikation inom en grupp även om de tillhör olika organisationer eller till och med nationer, något som kan effektivisera samarbete över gränser.

Genom att ABE är baserad på krypteringsteknik finns inget direkt beroende till centrala system. Detta medför att informationsobjekt kan krypteras och dekrypteras offline så länge informationsägare och mottagare i förväg erhållt korrekta nycklar. Oberoendet från centrala system möjliggör att informations-

objekt kan publiceras publikt, exempelvis på tredjeparts lagringsenheter, men även överföras till mottagare via exempelvis USB-minnen. ABE uppfyller på så sätt visionen om Obs (se avsnitt 2.1).

3.3 Obs-ABE-arkitektur

Ett viktigt resultat i projektet är den arkitektur som togs fram och som visar hur ABE kan bidra till att realisera Obs (Westerdahl, Hunstad & Mörnestedt 2014).

Arkitekturen, illustrerad i Figur 3, utgår från ett producent- och konsument-perspektiv på informationshantering, med tjänster som underlättar för säker kommunikation mellan producenter och konsumenter.

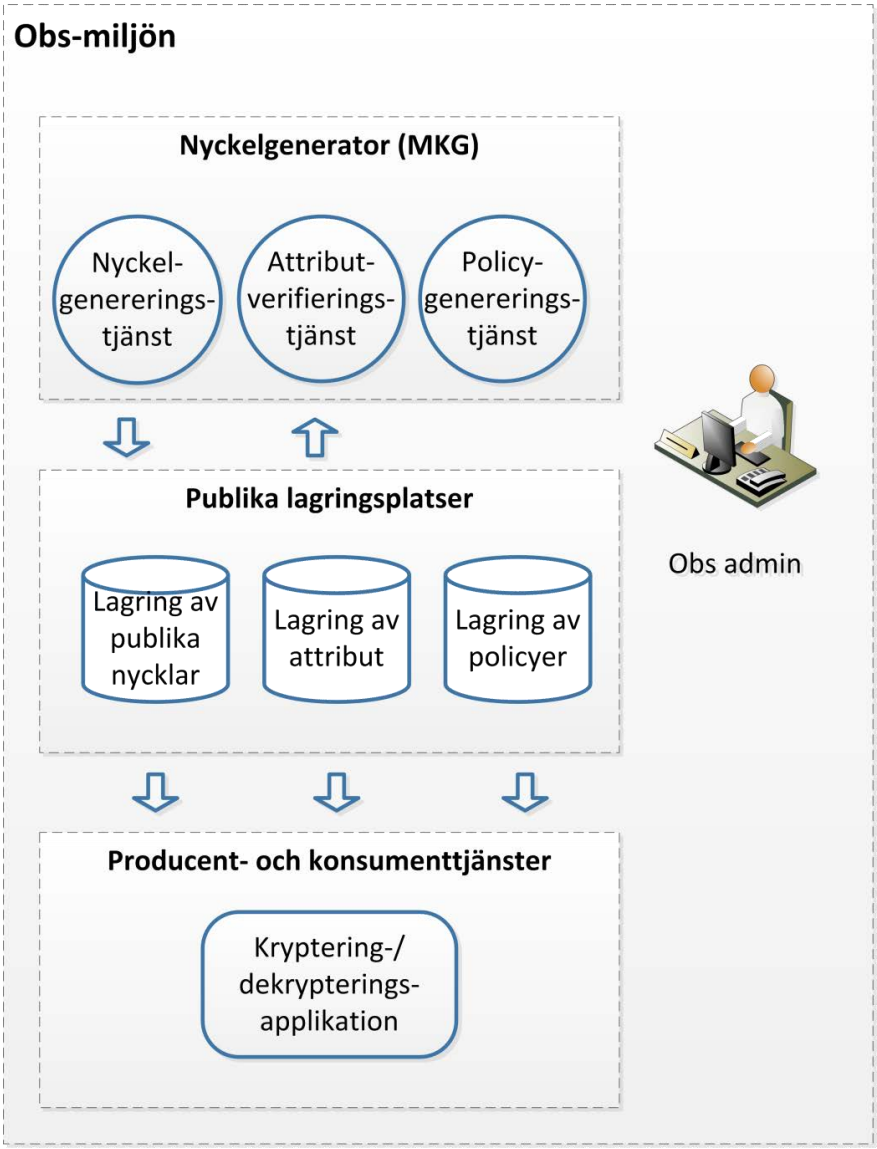
Obs-miljön består av fyra huvuddelar: en nyckelgenerator (på engelska ofta benämnd Master Key Generator, MKG), publika lagringsplatser, producent- och konsumenttjänster samt Obs-administratören (Obs admin).

Informationsproducenter skapar och tillhandahåller krypterade meddelanden. Informationskonsumenter är mottagare av krypterade meddelanden i behov av att kunna dekryptera dem. Konsumenterna är gruppmedlemmar och deras åtkomst till informationsobjektet beror på en policy.

Obs-administratören förvaltar Obs-miljön med ett särskilt ansvar att tillhanda-hålla (hemliga) dekrypteringsnycklar samt besluta hur åtkomst i olika situationer skall realiseras med attributstrukturer och policy.

Nyckelgeneratorn tillhandahåller tre tjänster: nyckelgenereringstjänst, attribut-verifieringstjänst samt policygenereringstjänst. Attributverifiering används när Obs-administratören tillhandahåller en uppsättning attribut för skapandet av en policy. Nyckelgeneratorn kontrollerar då att de tillhandahållna attributen ingår i den godkända uppsättningen attribut i den publika lagringsplatsen för attribut. Beroende på vald policyvariant av ABE, genereras hemliga dekrypteringsnycklar med hjälp av attributverifieringstjänsten eller policygenereringstjänsten.

Nyckelgeneratorn är av synnerligen stor vikt för ett ABE-baserat system, i och med att den skapar publika nycklar för kryptering av meddelanden. Då den även skapar dekrypteringsnycklar utgör den också en av ABE-systemens största sårbarheter. Av denna anledning väljer man normalt att placera nyckelgeneratorn offline från den operativa verksamheten i vilken producenter och konsumenter verkar. På grund av detta är det rimligt att tillhandahålla publika lagringsplatser för publika nycklar, attribut och policyer. Dessa lagringsplatser kan därmed avskärma nyckelgeneratorn och dess ingående tjänster samt minska dess exponering mot hot. Publika lagringsplatser är lokala resurser inom en Obs-miljö och ger åtkomst till information som kontinuerligt behövs för kommunikation.



Figur 3 Obs-ABE-arkitektur

I konkreta fall där en Obs-miljö realiseras kan miljön vara mera komplex än vad arkitekturen beskriver. I exempelvis koalitionssammanhang är det rimligt att multipla nyckelgeneratorer, multipla uppsättningar av producent- och konsumenttjänster samt multipla Obs-administratörer ingår. Vidare kan även konstruktioner som attributhierarkier krävas. Vad som ingår i respektive del av arkitekturen kan också vara betydligt komplexare än vad som illustreras här.

3.4 ABE-demonstrator

Inom projektet har en demonstrator utvecklats för att skaffa praktiska erfarenheter av ABE och för att kunna visa upp hur tekniken skulle kunna användas.

Den ABE-variant (Ciphertext-ABE) som implementerats i demonstratorn är en där policyn knyts till det krypterade meddelandet. Det innebär att en informationsproducent med utgångspunkt i en vald policy kan kryptera ett godtyckligt meddelande och sedan distribuera detta till en grupp av mottagare. Endast en användare som erhållit en dekrypteringsnyckel innehållande korrekta attribut kan dekryptera meddelandet. Demonstratorn innehåller programrutiner som realiserar en förenklad nyckelgenerator, en policygenereringstjänst och klienter för kryptering respektive dekryptering.

Policygenereringstjänsten används för att skapa en policy som sedan användas av klienten vid kryptering. Tjänsten möjliggör skapande av policyer genom att attribut som sedan tidigare är definierade visas som stöd i programrutinen för policygenerering. När användaren skall kryptera ett meddelande väljs vilken av de skapade policyerna som ska användas.

Demonstratorn har inte haft som ambition att visa en fullständig ABE-baserad lösning, utan fokus har varit på att demonstrera funktionaliteten hos de viktigaste delarna i en lösning där ABE används. Det kryptobibliotek som fungerade med ABE-programrutinerna i övrigt hade dock tydliga begränsningar, primärt på grund av begränsningar i det filformat som hanterades. Den realiserade policygenereringstjänsten medger å andra sidan möjligheten att realisera komplexa policyer med AND- respektive OR-funktioner. Ytterligare funktioner eller villkor utöver AND och OR ingår dock inte i demonstratorns policygenerering.

4 Säkerhetsegenskaper för attributbaserad åtkomstkontroll

Informationssäkerhetsområdet stödjer sig i stort på ett antal modeller för hur säkerhet uppnås eller bevaras. Modellerna är inte heltäckande och oftast beskrivna på en konceptuell nivå. Syftet med modellerna är att på ett övergripande sätt visa vilka egenskaper som utgör ett tillförlitligt system och därmed ett gott informationsskydd.

Ett policybaserat åtkomstsystem kan använda sig av säkerhetmodeller för att modellera en policy eller för att utvinna attribut som beskriver en säkerhetsmässig egenskap informationsägaren vill uppnå. Flera frågor uppstår kring denna målsättning, exempelvis; vilka attribut beskriver en säkerhetsegenskap? Och hur tolkas attributen på ett korrekt sätt?

I det här kapitlet beskrivs arbetet med att studera förhållandet mellan attribut och policyer för att upprätthålla en säkerhetsdomän. Arbetet har delvis genomförts i samarbete med Natoforskningsgruppen IST-114 Trusted Information Sharing for Partnerships.

4.1 Säkerhetsmodeller

I detta avsnitt beskrivs informationssäkerhetsmodeller som är relevanta för projektet.

4.1.1 CIA-triaden

Den flitigast använda säkerhetsmodellen är sannolikt CIA-triaden där CIA står för sekretess, riktighet och tillgänglighet (eng. confidentiality, integrity, availability). De ingående delarna kan enligt Terminologi för informationssäkerhet (SIS 2007) definieras som:

Sekretess	Ett informationsobjekt får inte göras tillgängligt eller avslöjas för obehöriga.
Riktighet	Information har inte förändrats av obehörig, av misstag eller av funktionsstörning.
Tillgänglighet	Ett informationsobjekt skall kunna utnyttjas i förväntad utsträckning och inom önskad tid.

Av dessa egenskaper är det sekretess som fått mest utrymme och också den egenskap som är bäst förstådd.

Det finns ett antal mer konkreta säkerhetsmodeller som beskiver hur främst sekretess men även riktighet skall vidmakthållas. Av dessa är sannolikt Bell-LaPadulas (1973) modell för sekretess och Bibas (1977) modell för riktighet mest kända.

Bell-LaPadula bevarar sekretessen genom att en användare med en given sekretessklarering endast får läsa uppgifter som befinner sig på motsvarande sekretessnivå eller lägre och endast skriva till samma sekretessnivå eller högre. Syftet är att en användare inte skall få tillgång till högre klassade uppgifter än vad den egna sekretessnivån medger och samtidigt skall inget informationsläckage uppstå genom att högre klassade uppgifter kan avslöjas i skrift på en lägre nivå.

Bibas modell är, i alla fall utseendemässigt, en rak motsats till Bell-LaPadulas modell. I Bibas modell bevaras en uppgifts riktighet genom att en användare endast får läsa uppgifter på sin egen nivå eller högre samt endast får skriva till sin egen nivå eller lägre.

Både Bell-LaPadula och Biba är ganska strikta modeller vilket har gjort dem svåra att hantera i praktiken. Behörighet baseras i huvudsak på användarens identitet och någon form av säkerhetsklarering. Detta är dock statiska attribut som är giltiga över tiden, oavsett hur omvärlden förändrar sig. En person är alltid samma person och en säkerhetsklarering är oftast personlig vilket innebär att den följer med användaren så länge den är giltig, även om denne byter arbets-uppgifter. Här uppstår begränsningar då omgivande faktorer även borde kunna påverka åtkomstbeslutet.

Tillgänglighet har alltsomoftast haft en underordnad betydelse, i alla fall i militära informationssystem där bevarande av sekretess är överordnat de flesta andra egenskaper. Tillgänglighet skiljer sig mot sekretess och riktighet genom att mer vara något som uppnås på systemnivå. Det är svårt för informationsobjektet att själv påverka sin tillgänglighet.

Inom enskilda branscher och tillämpningar har tillägg gjorts för att täcka egenskaper som CIA-triaden inte gör. Nedan följer några exempel på fylligare modeller.

4.1.2 Ledningssystem för informationssäkerhet

Ledningssystem för informationssäkerhet (Lis) (SIS 2014) har utvecklasts genom att sammanföra flera ledningssystemsstandarder i syfte att ge ett mer enhetligt införande och enhetlig drift rörande informationssäkerhet. Lis använder utöver sekretess, riktighet och tillgänglighet även begrepp som ansvarig (eng. accountability), oavvislighet (eng. non-repudiation), äkthet (eng. authenticity) och pålitlighet (eng. reliability).

4.1.3 Parkers hexad

En utveckling av CIA-triaden har tagits fram av Donn Parker (2010). Parkers främsta invändning mot CIA-triaden var att den inte tar hänsyn till användare eller förövare utan enbart fokuserar på att beskriva skyddsegenskaper. Parkers kompletterande egenskaper återfinns i Tabell 1.

Tabell 1 Parkers hexad.

CIA-element	Parkers tillägg
Sekretess	Innehav
Riktighet	Äkthet
Tillgänglighet	Användbarhet

Sekretess kopplas oftast till att bevara uppgifter från obehörig exponering i någon mening. Med innehav (eng. possession) avser Parker skydd av uppgifter som innehas av någon obehörig, oavsett om uppgifternas eventuella sekretess är röjd eller ej.

Riktighet avser att information är oförändrad när den når en mottagare. Det säger dock inget om informationens äkthet (eng. authenticity) – det vill säga informationens ursprung.

Att information är tillgänglig behöver inte betyda samma sak som att informationen är användbar (eng. utility). Tillgänglig information i ett mindre användbart filformat kan mycket väl ge mottagaren tillgång till informationen men användbarheten är låg.

Parkers modell har debatterats inom informationssäkerhetsdomänen men inte blivit allmänt vedertagen.

4.1.4 X.800

Referensmodellen för datakommunikation Open System Interconnection (OSI), framtagen av International Telecommunication Union Telecommunication Stanardization Sector (ITU-T), beskriver hur olika lager inom en dator samverkar för att kommunicera med andra datorer. X.800 (ITU-T 1991) är en utökning av OSI-modellen som närmare beskriver modellens generella säkerhetsegenskaper. Egenskaperna beskrivs av de tjänster som bör ingå i ett nätverk:

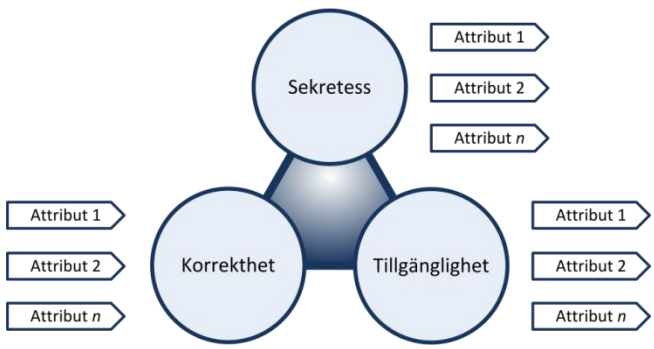
- Autentisering
- Åtkomstkontroll

- Datasekretess
- Datariktighet
- Oavvislighet

Vart att notera i X.800 är att tillgänglighet inte ingår utan anses vara ett resultat av nätverkets design, till exempel genom att bygga nätverket så att överbelastningsattacker (eng. Denial-of-Service) försvåras.

4.2 Attribut för säkerhetsmodeller

När en säkerhetsmodell omsätts i ett verkligt informationssystem sker detta dels genom teknisk design och implementation, dels genom regelverk i form av policyer. Design och implementation i form av hårdvara och mjukvara är mer statiska i sin karaktär vilket gör dem svåra att anpassa efter nya förutsättningar. Detsamma gäller mindre hårda byggstenar såsom informationsmodeller. Idéer om, och yttre påverkan på, hur informationssystem bör användas kan däremot påverkas genom arbetsprocesser och policyer. Inom projektet har policyer varit mest i fokus.



Figur 4 Relationen mellan en modell och attribut.

En policy för åtkomstbeslut beskriver vad som krävs för att en användare skall få tillgång till ett informationsobjekt. Det finns flera olika typer av åtkomstkontroll, exempelvis åtkomstkontrollistor, rollbaserad åtkomstkontroll eller attributbaserad åtkomstkontroll. Gemensamt för dem alla på en högre nivå är att någon typ av uppgift behöver presenteras för den instans som beslutar om åtkomsten. Denna instans rättar sig i sin tur efter en uppsättning regler. Alltså, en användare anger (minst) sin identitet och beslutsinstansen kontrollerar presenterade attribut mot uppsatt regelverk, det vill säga en policy. Relationen mellan attribut och modell illustreras av figur 4.

Attribut kan uttrycka en värdering såsom en informationssäkerhetsklass, vilken ofta kan sättas in i en skala. Sådana attribut bär med sig en statisk värdering av innehållet vilken i sin tur värderas gentemot en policy innan åtkomst medges. Ett alternativ är att låta attribut uttrycka objektiva värden, det vill säga beröra informationsobjektets innehåll och låta policyer avgöra det kontextuella skyddsvärdet.

4.2.1 Attribut med värdering

Värden på attribut kan uttryckas på flera sätt. Ett sätt är att låta attributets utfallsrum utgöras av en värderande skala. Ett typiskt exempel på en värderande skala är de värden ett attribut för sekretess skulle kunna anta, från sekretessklassificerat till hemlig/top secret. En mer generisk skala men som också kan uttrycka konsekvens av ett misslyckande att upprätthålla den satta bedömningen är av typen låg, mellan och hög enligt Federal Information Processing Standards (FIPS) (2004). FIPS skala används för att beskriva vilken påverkan ett bortfall av respektive sekretess, riktighet och tillgänglighet får i en verksamhet (National Institute of Standards and Technology (NIST) 2008).

I och med att skalor utgör en bedömning måste denna uppdateras efterhand. En sådan värdering sker oftast när ett informationsobjekt efterfrågas. Processen är i dagsläget oftast manuell och svår att överföra till ett datorsystem i och med att bedömningen är subjektiv och att den som utför bedömningen oftast endast har ett grovt regelverka att följa. Detta medför att en bedömning kan variera från person till person.

Fördelen med fasta värden för attribut är att det är enklare att skapa policyer för åtkomst i och med att en värdering av informationsobjektet redan finns.

4.2.2 Attribut utan värdering

Ett alternativ till attributvärden baserade på skalor är statiska och icke-värderande attribut. Ett objektivt attribut uttrycker något som inte ändras, exempelvis födelseår. Attributet födelseår med värdet 1971 ger ett system möjlighet att lätt räkna ut vilken ålder personen som attributet beskriver har men mer säger attributvärdet inte. Systemet som använder attributet kan dock ha en policy som tolkar attributvärdet i en viss kontext och avgör om personen ifråga är för ung eller för gammal. Oavsett tolkning så förändras inte attributet över tiden men uppfattningen om attributvärdet kan förändras.

Objektiva attributvärden ställer stora krav på hur en policy utformas. Idealt skall en policy uttrycka den aktuella säkerhetsmässiga hållningen en organisation har antagit. En sådan hållning är dock beroende av en kontext vilket kan göra en detaljerad policy svårt att upprätta och kanske framförallt svår att implementera i ett automatiserat förlopp med rimlig assurans. Å andra sidan så finns någon form

av policy när en manuell bedömning görs även om den till viss del är personlig. Alltså borde rimliga mätvärden gå att identifiera och reglera. Den avgörande frågan är kanske hur lång tid det tar att upprätta eller förändra en detaljerad policy, inte hur komplex den är.

En åtkomstpolicy kan baseras på både värderingar och objektiva värden. Det finns ett behov av mer automatiska bedömningsfunktioner i framtiden och en tydlig informationsmärkning är en förutsättning för detta.

4.3 Riktighet och tillgänglighet

En fråga som är intressant att ställa är om riktighet och tillgänglighet kan vara egenskaper som bör påverka ett åtkomstbeslut på samma sätt som sekretess gör det. Den här frågeställningen har studerats inom projektet och i samarbete med Natoforskningsgruppen IST-114 Trusted Information Sharing for Partnerships. Arbetet inom IST-114 beräknas resultera i en rapport till Nato Science & Technology Organization (NATO STO) under 2015. Nedan ges en sammanfattning av arbetet inom IST-114 avseende riktighet och tillgänglighet.

4.3.1 Riktighet

För vissa typer av uppgifter är riktigheten viktigare än att uppgiften hålls hemlig. För exempelvis styrsignaler, mätvärden och varningssignaler kan exponering inte påverka mottagaren medan riktigheten ofta är kritisk.

Till skillnad från sekretess, där innehållet i uppgiften skall skyddas från exponering, är det svårt att skydda ett informationsobjekt från förändring eller förvanskning. Riktighetsfunktioner syftar därför till att upptäcka om en förändring har skett.

En strikt tolkning av riktighet ur ett informationssäkerhetsperspektiv är att en konsument skall erhålla det objekt som efterfrågats och att det inte har förändrats eller på annat sätt påverkats under transporten till mottagaren. När riktighet diskuteras med dess engelska ord (integrity) och med Bibas modell i åtanke, är det lätt att tankar som tilltro (eng. trust) till uppgifter uppkommer. I en sådan diskussion skulle integritetskrav kunna handla om att endast personer på en viss enhet eller med en viss behörighet få bidra med uppgifter (Li, Mao & Zdancewic 2003). Om inte, kan riktigheten i informationsobjektet försvagas beroende på att de som ges behörighet att förändra objektet saknar kunskap om innehållet och därmed negativt påverkar det. Här inkluderas alltså riktighetspåverkan rörande legitim användning.

Om information blir otillgänglig kan tillgängligheten normalt återfås vid ett senare tillfälle. Men när information läckt ut har sekretessen gått förlorad och det är normalt omöjligt att göra det hela ogjort och att återfå sekretessen. Vad gäller

riktighet går information ofta förlorad för evigt när den förvanskats eller förstörts, även om backuprutiner till viss del kan understödja här.

Hittills har riktighet beskrivits som något som endast är av intresse för mottagaren. Det finns dock två sidor av myntet. Det är mottagaren som vill säkerhetsställa att hela det begärda informationsobjektet har överförts och att det inte har förändrats under transporten. Avsändaren däremot har inget större behov av riktighet i det här fallet. Ur ett verksamhets- eller trovärdighetsperspektiv kan det vara annorlunda. Det finns en variant där det är producenten av information har ett större behov av riktighet än mottagaren, nämligen i de fall där producenten delar med sig av material som de vill vara säkra på att det inte förändras utan deras medgivande. Syftet med ett sådant skydd är att säkerhetsställa att producenten av ett informationsobjekt inte blir tillskriven ansvar för mer än vad denne väljer att dela med sig av. Här finns alltså en koppling till äkthet.

4.3.2 Tillgänglighet

Tillgänglighet har inom informationssäkerhetsområdet i huvudsak varit en fråga om systemkrav och till viss del serviceavtal. Det är svårt för ett informationsobjekt att själv säkerställa tillgängligheten. Ett informationsobjekts tillgänglighetsattribut skulle dock kunna fungera som krav på det system objektet anländer till. Som kravställare kan inte objektet garantera att kraven efterlevs men så länge informationsobjektet används inom en organisation eller koalition ligger efterlevnad av kravet i allas intresse.

Tillgänglighet kan kategoriseras som fysisk, logisk eller villkorslös. Fysisk tillgänglighet betyder att informationsobjektet finns fysiskt tillgängligt hos konsumenten. På så sätt är objektet alltid tillgängligt. Den logiska tillgången är den man oftast tänker på rörande informationssystem, nämligen förmågan att kunna hämta uppgifter från en lagringsplats när behovet uppstår. En villkorslös tillgänglighet tar ett lite annat perspektiv och omfattar inte bara förmågan till åtkomst utan även vilket format som informationsobjektet är i. Dessutom måste formatet vara något som de flesta system rimligen kan förstå, exempelvis en textfil.

Nedan följer några exempel på hur tillgänglighet måste hanteras i Obs-visionen.

Krav på tillgänglighet. Ett informationsobjekt kan vara viktigt för en större del av användarna i ett system eller utgöra uppgifter till ett subsystem som är essentiella för dess funktion. Ett sådant informationsobjekt kan behöva lagras i system med hög tillgänglighet, korta svarstider, externa lagringsplatser, etcetera.

Undantag från säkerhetspolicy. Tillgänglighet är oftast ett problem mellan informationssystem och en användare som vill konsumera information. En tillämpning av tillgänglighetsattribut kan vara att visa på undantag som får göras

gentemot gällande säkerhetspolicy, i syfte att uppnå högre tillgänglighet för kritiska uppgifter. Exempel på sådana undantag skulle kunna vara att skicka uppgifter över en oskyddad kanal om den skyddade kanalen inte är tillgänglig, givetvis under förutsättning att det är kritiskt att uppgiften kommer fram snabbt.

Krav på mottagande system. Uppgifter som (exempelvis) måste vara tillgängliga kan ställa krav på ett mottagande system så att informationsobjektet när det anländer vidmakthåller graden av tillgänglighet. Ett sådan här lösning kräver att sändande och mottande system kan förhandla med varandra enligt den nivå som anges av informationsobjektet innan det skickas iväg.

5 Kunskapsöverföring och internationella kontakter

I det här kapitlet redovisas aktiviteter som bidragit till kunskapsöverföring till projektet från omvärlden samt aktiviteter där syftet både varit överföring och inhämtning.

5.1 Seminariedagar

IT-säkerhetsprojekten inom FoT genomför årligen en seminariedag där resultat från det gångna året presenteras samt möjlighet ges att diskutera den framtida inriktningen av projekten. Seminariedagarna har genomförts sedan 2008 och har i huvudsak varit halvdagshändelser.

Syftet med seminariedagarna är att sprida kunskap om vad IT-säkerhetsprojekten inom FoT gör men framför allt att skapa en dialog mellan Totalförsvarets forskningsinstitut (FOI), Försvarsmakten och Försvarets materielverk (FMV) men även Försvarshögskolan (FHS).

Under seminaridagen 2014 utökades konceptet genom att inkludera föredrag från Försvarsmakten och därmed göra det till en heldagshändelse.

5.2 Internationellt samarbete

Medlemmar i projektet har deltagit i ett antal forskningssamarbeten inom Nato. Inom ramen för projektet har även ett arbetsmöte genomförts med Air Force Research Laboratory (AFRL) i USA. Dessa samarbeten beskrivs närmare i detta avsnitt.

5.2.1 IST-096 Information Assurance / Cyber Defence Research Framework

FOI har genom projektet Objektbaserad säkerhet deltagit som medlem i forskningsgruppen IST-096 Information Assurance / Cyber Defence Research Framework. IST-096 syftar till att utveckla ett ramverk för forskning inom områdena assurans och cyberförsvar.

Arbetet har genomförts med utgångspunkt från den preliminära forskningsplan som togs fram i en förstudie, tillämpning av ARMOUR (Sawilla & Wiemer

2011) samt NATO Communication & Information Agencys (NCIA) arbete med förmågenedbrytning av informations- och kommunikationsteknik (IKT)[2].

ARMOUR har anpassats efter gruppens behov och kallas nu för Prototyping Environment (PE) och beskriver en utvecklingsmiljö där parter kan samarbeta om utveckling kring cyberförsvarsprodukter. IST-096 har tagit fram ett antal scenarier där en PE används för samarbete och utveckling av produkter inom cyberförsvar och informationsassurans.

IST-096 har aktivt deltagit att utveckla NCIA:s arbete samt organiserat ett möte med industrirepresentanter i syfte att få återkoppling på ramverkets mognad och hur det kan komma att accepteras av industrin om det blir en standard inom Nato. En rapport om industrimötet är under produktion (Nato 2014).

Gruppens slutresultat avseende ett ramverk för forskning inom cyberförsvar kopplar samman mognadsmodellen Technology Readiness Level (TRL) med de aktiviteter som genomförts inom gruppen.

IST-096 förväntas publicera en rapport om PE och en rapport om forskningsramverket genom Natos forskningsorganisation Science & Technology Organization (NATO STO) under 2015.

5.2.2 IST-111 Information Assurance and Cyber Defence

Information Assurance and Cyber Defence (Nato 2012) var ett Natosymposium som genomfördes i Koblenz, Tyskland 24-25 september 2012. En projekt-medarbetare deltog i förarbetet till symposiet som medlem i programkommittén.

5.2.3 IST-114 Trusted Information Sharing for Partnerships

IST-114 Trusted Information Sharing for Partnerships har en bred ansats. Arbetet har i huvudsak två inriktningar; design av en Information Exchange Gateway (IEG) samt studie av riktighet och tillgänglighet som egenskaper för åtkomstkontroll.

Natos utveckling av IEG delas in i fyra scenarier; kommunikation mellan A) olika Nato Secret-nätverk, B) Nato Secret-nätverk och nationella Secret-nätverk, C) Nato Secret-nätverk och Nato-missionsnätverk, samt D) Nato Secret-nätverk och andra organisationers nätverk[3] (Nato 2008; Deep Secure 2014). Ibland omnämns även ett femte scenario (E) för kommunikation mellan Nato Secret-nätverk och Internet i allmänhet. IST-114 har inriktningen scenario D.

[2] eng. Information and Communications Technology (ICT).
[3] Med andra organisationer avses här exempelvis internationella organisationer, icke-statliga organisationer, icke-Natonationer, mm.

IST-114:s andra inriktning är mot informationsegenskaper för säkerhet. Målsättningen är att identifiera hur riktighet och tillgänglighet kan användas för att förbättra ett åtkomstbeslut. Arbetet tar sin utgångspunkt i IST-068 XML in Cross Domain Security Solutions, samt i målsättningen för NATO Communication & Information Agency (NCIA) Content Protection and Release (CPR). Projektet IST-068 syftade till att införa en märkning för sekretess inom ramen för eXtended Markup Language (XML), utan att ställa krav på förändring i mottagande system. Det har inte publicerats en officiell rapport från gruppens arbete men Forsvarets forskningsinstitutt (FFI), som deltog i arbetet har publicerat en rapport med resultat (Haakseth 2012).

NCIA CPR (Wrona & Oudkerk 2013) är en åtkomstkontrollfunktion som delar upp åtkomstkontroll i två delar; en som hanterar hur information lagras (protection) och en som hanterar kriterier för när information släpps till den som begär den (release).

Det huvudsakliga intresset angående IST-114 för projektet Objektbaserad säkerhet faller inom frågeställningen om egenskaper för riktighet och tillgänglighet. Resultatet av samarbetet beskrevs i kapitel 4.

5.2.4 Workshop med AFRL

I april 2013 genomfördes en workshop med AFRL. Syftet med workshopen var att identifiera möjliga samarbetsområden inom ämnesområdet cybersäkerhet. Informationsutbyte med AFRL har även skett i samband med Senior National Representative-möten (SNR-möten).

De intresseområden som diskuterats är objektbaserad säkerhet, cyberövningar, pålitliga plattformar samt cybersäkerhet i obemannade farkoster.

5.3 Finansiering av EU-uppdrag

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).[4] FIDELITY är en del av Europakommissionens sjunde ramprogram[5] och som sådant finansieras det till 75 % av EU medan resten medfinansieras av deltagarna.

FIDELITY-projektets uppgift är att analysera brister och sårbarheter i livscykeln för elektroniska pass i syfte att rekommendera förbättringar och utveckla lösningar. Projektet ska presentera lösningar för att förbättra processen för att upprätta ett pass, förbättra säkerheten i elektroniska pass, utöka passens

[4] http://foi.se/fidelity (2013-11-13)
[5] http://cordis.europa.eu/fp7/home_en.html (2013-11-12)

användbarhet, stärka rutiner kring försvunna och stulna pass samt säkerställa individens integritet.

Elektroniska pass är avsedda att användas i en internationell kontext. Själva passen har utöver de visuellt läsbara uppgifterna även ett chip av typen Radio Frequency Identification (RFID), där de visuella uppgifterna är duplicerade tillsammans med vissa tillagda biometriska uppgifter. För att identifiera förfalskningar måste uppgifterna på RFID-chipet verifieras, vilket sker med stöd av digitala certifikat. Tekniken för detta är beprövad, men på grund av nationella intressen varierar tillämpningen från nation till nation. Erfarenheter från detta arbete ökar förmågan att förstå de behov som kan uppkomma när säkerhetsfunktioner behöver samarbeta eller kommunicera i exempelvis en koalition.

Säkerhetsarbetet inom FIDELITY utgår från en hotanalys. I processen att omsätta hotanalysen till krav på säkerhetsfunktioner har flera erfarenheter dragits avseende hur sådana krav bör formuleras på ett tydligt sätt. Olika intressenters behov rörande passhantering behöver vägas in, vilket utgör en intressant och betydande utmaning vid utvecklingen av relevanta lösningar. FIDELITY-projektet har gett värdefulla erfarenheter i avvägningen mellan behov, krav och möjliga lösningar för komplexa samverkande internationella system. För att nå eftersträvad tilltro till passhanteringsprocessen är det synnerligen viktigt att såväl helheten som delarna av ett sådant komplext och samverkande system kan bedömas vara pålitliga. FOI bidrar till arbetet inom områdena:

- Behovs- och protokollanalys
- Vidareutveckling av certifikathantering
- Systemtilltrohöjande åtgärder
- Bättre och effektivare metoder för verifiering av identitet.

FOI:s deltagande i FIDELITY-projektet avslutas under början av 2015 medan FIDELITY-projektet som helhet avslutas under början av 2016.

6 Slutsatser

Objektbaserad säkerhet (Obs) är en vision. Som sådan har den på senare år blivit mer realistisk, främst genom en mer attributinriktad åtkomstmetodik. Attributbaserad åtkomstkontrollvarianten ABAC är fortfarande den mest effektiva och mogna metoden för att erhålla en finmaskig åtkomstkontroll. Svagheten med ABAC är dock att den kräver uppkoppling mot en server. Attributbaserad kryptering (ABE) har visat sig vara en viktig kandidat för att uppnå Obs-visionen i en offlinemiljö genom att attribut och åtkomstpolicy är inbyggda i krypteringen av informationsobjektet.

Användning av mer finmaskiga åtkomstpolicyer inom en verksamhet kan ge högre tillgänglighet till information, vilket i sin tur förhoppningsvis ger en effektivare verksamhet. Vanlig åtkomstkontroll kan förstärkas med ABAC men ABAC sträcker sig inte utanför de egna systemen. ABE kan på sikt vara en lösning där en åtkomstpolicy kan följa med ett informationsobjekt utanför de egna systemen, exempelvis när ett informationsobjekt skickas med mejl eller delas via ett USB-minne.

En policystyrd verksamhet har större möjlighet att åstadkomma en högre grad av automatiska åtkomstkontroller. Dagens informationstakt är hög och morgondagens kommer gissningsvis att vara ännu högre. En manuell hantering av informationsutbyte över exempelvis nationsgränser i koalitioner kommer att behöva automatiseras för att klara av utbytesbehoven.

Sekretess är fortfarande den egenskap som får mest uppmärksamhet avseende skydd av informationsobjekt. Det är dock värdefullt att studera hur andra egenskaper kan komplettera sekretessen som urvalsfaktor för åtkomst och spridning av information. Riktighet och tillgänglighet är viktiga inte enbart för mottagaren av informationen utan kan även vara viktiga för en avsändare.

Visionen med objektbaserad säkerhet närmar sig en verklig lösning alltmer. Inom ramen för projektet Objektbaserad säkerhet har genom ABE en metod för att knyta säkerhetsmässiga egenskaper till ett informationsobjekt påvisats. ABE kan inom vissa gränser även bevara skyddet av informationsobjektet när det anlänt till mottagaren, i alla fall så länge mottagaren väljer att använda det skyddade informationsobjektet för vidare kommunikation.

Referenser

Alvegård, L. (1994). Arkaisk babylonisk matematik: Talpjäser och lerbollar, *Teknik & Naturvetenskap*, 2.

Bell, D.E. & LaPadula, L.J. (1973). *Secure Computer Systems: Mathematical Foundations* (MTR-2547, vol. I). MITRE.

Biba, K. (1977). *Integrity Considerations for Secure Computing Systems* (MTR-3153, rev. 1). MITRE.

Deep Secure (2014). *Implementing Deep-Secure guards in NATO Information Exchange Gateways*. http://www.deep-secure.com/wp-content/uploads/2014/04/IEG-Paper-01-v1.01.pdf [2014-11-27]

Federal Information Processing Standards (FIPS) (2004). *Standards for Security Categorization of Federal Information and Information Systems* (FIPS PUB 199). Gaithersburg: NIST.

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

Hunstad, A.G., Gustafsson, T., Karlzén, H., Mörnestedt, F., Westerdahl, L. (2012). *Objektbaserad säkerhet – Behov och möjligheter* (FOI-R--3484--SE).

ITU-T (1991). *Security architecture for Open Systems Interconnection for CCITT applications*.

Li, P., Mao, Y. & Zdancewic, S. (2003). Information Integrity Policies. I *FAST'03, Proceedings of the workshop on formal aspects in security & Trust*. Pisa, Italien september 2003, ss. 53-70.SS-ISO/IEC 17799

Nato (2008). *Guidance Document On The Implementation Of Gateways For Information Exchange Between NATO CIS and External CIS* (AC/322-D(2005)0054-REV2).

Nato (2014). *Workshop on Cyber Security Capabilities, The Hague, The Netherlands - Publication Announcement*. 16 januari. https://www.cso.nato.int/page.asp?ID=1722 [2014-11-19]

NATO Science and Technology Organization (NATO STO)(2012). *Symposium on Information Assurance and Cyber Defence* (STO-MP-IST-111). Koblenz, Tyskland 24-25 september 2012. https://www.cso.nato.int/pubs/rdp.asp?RDP=STO-MP-IST-111 [2014-11-20]

National Institute of Standards and Technology (NIST) (2008). *Volume I: Guide for Mapping Types of Information Systems to Security Categories* (NIST SP 800-60). Gaithersburg: NIST.

Parker, D. (2010). Our excessively simplistic information security model and how to fix it. *ISSA Journal*, 8(7), ss. 12-21.

Pettersson, J.S. (1991). *Critique of evolutionary accounts of writing* (RUUL 21). Uppsala Universitet, institutionen för lingvistik och filologi. Uppsala: Uppsala Universitet.

Robinson, A. (1996). *Skriftens historie*. Oslo: Grøndahl Dreyer.

Schmandt-Besserat, D. (1982). How writing came about. *Zeitschrift für Papyrologie und Epigraphic*, (47), ss. 1-5.

Sawilla, R.E. & Wiemer, D.J. (2011). Automated computer network defence technology demonstration project (ARMOUR TDP): Concept of operations, architecture, and integration framework. I *HST'11, 2011 IEEE International Conference on Technologies for Homeland Security.* Waltham (MA), USA 15-17 november 2011, ss. 167 - 172. DOI: 10.1109/THS.2011.6107865

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

Swedish Standards Institute (SIS) (2014). *ISO/IEC 27000:2014 Ledningssystem för informationssäkerhet - Översikt och terminologi* (ISO/IEC 27000:2014, IDT). Stockholm: SIS.

Westerdahl, L., Hunstad, A.G. & Mörnestedt, F. (2014). *Object-Based Security with Attribute-Based Encryption: A Feasibility Study* (FOI-R--4002--SE). Stockholm: Totalförsvarets forskningsinstitut.

Wrona, K. & Oudkerk, S. (2013). Content-Based Protection and Release Architecture for Future NATO Networks. In *MILCOM 2013, Military Communications Conference*. San Diego, USA 18-20 november 2013. DOI: 10.1109/MILCOM.2013.44

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