Teknik för IT-säkerhet

Slutrapport

JACOB LÖFVENBERG

FOI-R--4496--SE
ISSN 1650-1942 December 2017

Jacob Löfvenberg

Teknik för IT-säkerhet

Slutrapport

Titel	Teknik för IT-säkerhet – Slutrapport
Title	Methods for IT Security – Final Report
Rapportnr/Report no	FOI-R--4496--SE
Månad/Month	December
Utgivningsår/Year	2017
Sidor/Pages	20 p
Kund/Customer	Försvarsmakten
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Ledning och MSI
Projektnr/Project no	E72677
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem
Exportkontroll	Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen.

Detta verk är skyddat enligt lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk, vilket bl.a. innebär att citering är tillåten i enlighet med vad som anges i 22 § i nämnd lag. För att använda verket på ett sätt som inte medges direkt av svensk lag krävs särskild överenskommelse.

This work is protected by the Swedish Act on Copyright in Literary and Artistic Works (1960:729). Citation is permitted in accordance with article 22 in said act. Any form of use that goes beyond what is permitted by Swedish copyright law, requires the written permission of FOI.

Sammanfattning

Denna rapport beskriver det arbete som utförts inom ramen för FoT-projektet *Teknik för IT-säkerhet*, åren 2015–2017, och adresserar frågor om att hitta säkerhetslösningar som möjliggör effektiv IT-användning. Projektet har huvudsakligen bedrivits i form av ett antal separata studier inom området. Rapporten sammanfattar resultaten från dessa studier och beskriver kortfattat övriga aktiviteter i projektet.

Nyckelord: IT-säkerhet, assurans, formella metoder

Summary

This report describes the work that has been done within the FoT project *Teknik för IT-säkerhet* (Technology for IT security) during 2015–2017. It addresses questions about identifying security solutions enabling effective IT usage. The project has mainly been done in the form of a number of separate studies within the area. The report summarizes the results of these studies and shortly describes other activities in the project.

Keywords: IT security, assurance, formal methods

Innehållsförteckning

1 Inledning

Försvarsmakten använder allt fler IT-system och i en allt större omfattning. Denna användning resulterar i risker som behöver hanteras av effektiva säkerhetslösningar. Sådana lösningar kan vara tekniska, administrativa eller organisatoriska. I FoT-projektet *Teknik för IT-säkerhet* har fokus legat på att utvärdera tekniska metoder för att skapa säker hantering av IT-system. Detta dokument är en slutrapport för projektet och sammanfattar verksamheten och resultaten i projektet.

Projektet har bedrivits i ett antal parallella spår och gjort flera relaterade studier snarare än att göra ett enda sammanhängande arbete som pågått under hela projektets livslängd. Detta har tillåtit en hög grad av anpassningsbarhet och möjliggjort att med relativt kort varsel studera frågor som kommit upp inom FOI:s kontaktnät i Försvarsmakten.

Projektet har haft fokus på att identifiera och undersöka IT-säkerhetshöjande tekniker och metoder, samt på att utvärdera Försvarsmaktens behov och nytta av sådana tekniker.

I FoT-planen framgår att följande frågeställningar ska beaktats i projektet:

- Vilka IT-säkerhetstekniker och -metoder finns som kan användas för att inom Försvarsmakten möjliggöra effektiv IT-användning med bibehållen IT-säkerhet?
- Vilka IT-säkerhetstekniker och -metoder finns som kan möjliggöra användning av icke-militära informationssystem för militärt bruk?
- Hur kan identifierade IT-säkerhetstekniker enligt ovan nyttjas inom Försvarsmakten?

För Försvarsmaktens del innebär effektiva, IT-säkerhetshöjande tekniker att fler och bättre IT-baserade verktyg kan användas utan att IT-säkerheten minskar. Med bättre hjälpmedel blir den verksamhet som stöds av hjälpmedlen effektivare, vilket innebär att verksamheten erhåller en förbättrad förmåga.

1.1 Aktiviteter i projektet

Den största delen av projektets arbete har handlat om att genomföra forskningsstudier relaterade till tekniker och metoder för IT-säkerhet i Försvarsmakten. Processen har varit att FOI har fångat upp frågor och idéer som lämpar sig för studier och därefter, efter att ha dialogiserat frågeställningen med relevanta personer i Försvarsmakten, genomfört studierna och återfört resultaten till de intressenter som identifierats under beredningen och genomförandet.

Ett projektspår som fortlevt under hela treårsperioden är studier av formella metoder för att verifiera korrekthetsegenskaper hos programkod. Denna inriktning var beskriven i FoT-planen och har därför varit given redan från projektets start.

En del av projektet har handlat om att bedriva omvärldsanalys i syfte att upprätthålla en övergripande bild av vilka IT-säkerhetstekniska frågor som är aktuella i Försvarsmakten och vilken forskning som bedrivs i landet och internationellt. Denna omvärldsanalys har genomförts i form av ministudier som var och en belyser någon aktuell, relevant aspekt av frågan. I FoT-planen pekas objektbaserad säkerhet ut specifikt som något som ska ingå i omvärldsanalysarbetet, varför även detta har behandlats under projektets samtliga tre år.

Utöver studierna har projektet organiserat seminarier om försvarsrelaterade IT-frågor, först under namnet IT-säkerhetsdagen, sedan under namnet IT-försvarsdagen. Syftet med dessa seminarier har varit dels att sprida kunskap om FOI:s verksamhet inom IT-säkerhets-området, dels att skapa en arena där myndighetspersonal kan träffas och utbyta erfarenheter.

Slutligen har projektet finansierat FOI:s deltagande i Natogruppen IST-114 och under 2015 motfinansierat FOI:s deltagande i EU-projektet Fidelity.

1.2 Rapportstruktur

Rapportens fortsatta disposition är som följer:

- kapitel 2 beskriver de forskningsstudier som genomförts,
- kapitel 0 redogör för de omvärldsstudier som genomförts,
- kapitel 4 beskriver seminarieverksamheten,
- kapitel 5 ger en kort beskrivning av deltagandet i Natogruppen IST-114,
- kapitel **Error! Reference source not found.** innehåller en kort diskussion,
- kapitel 7 innehåller en sammanställning av de publikationer som gjorts inom ramen för projektet.

Beskrivande text om projektets olika delar har återanvänts från de publikationer som gjorts tidigare i projektet.

2 Studier

I detta kapitel beskrivs de studier som genomförts inom ramen för projektet. I kapitel 7 finns fullständiga referenser för de rapporter som hänvisas till nedan.

2.1 Verktyg för att åstadkomma pålitlig programvara

Studien *Verktyg för att åstadkomma pålitlig programvara*[1] bygger huvudsakligen på en litteraturstudie som resulterade i en sammanställning av ett urval allmänt tillgängliga verktyg som används för att åstadkomma pålitlig programvara. Syfte med studien var att ge en översikt av aktuell status på forskningen inom området pålitlig programvara. Denna studie avslutar det arbete som påbörjades i det tidigare projektet Pålitliga IT-plattformar, som av administrativa skäl avbröts i förtid.

De olika klasser av verktyg som beskrevs av (1) formella metoder, (2) standarder, (3) organisationer, (4) säkra programspråk, (5) sårbarhetsförutsägelse och (6) säkra operativsystem. Dessa verktygsklasser presenterades översiktligt och förklarades på en grundläggande nivå.

Slutsatserna i studien var att forskning och utveckling rörande verktyg för att åstadkomma pålitlighet i programvara har ökat på senare tid, men att den ännu inte nått tillräcklig mognadsgrad för att slå igenom fullt ut i produktionsledet. Användning av standarder och certifiering är vanligt förekommande. Programvaruutvecklingsverktyg baserade på formella metoder ansågs visa lovande resultat, men kräver i de flesta fall fortfarande speciallösningar för att vara användbara.

2.2 Formella metoder

Det vanligaste sättet att hitta och korrigera fel i mjukvara är testning. I kombination med god utvecklingsmetodik som ger få fel under utvecklingen går det på detta sätt att nå hög kodkvalitet som ger god tillgänglighet till de funktioner som mjukvaran erbjuder. För att lyckas väl krävs dock ett noggrant och mödosamt arbete.

Säkerhetsmässig korrekthet hos mjukvara är ur en principiell synvinkel inte skild från korrekthet i allmänhet, men i praktiken blir skillnaden stor. En angripare kan välja sitt beteende så att den mest ogynnsamma situationen för mjukvaran inträffar, en situation som utan en tänkande angripare skulle ha en försumbar sannolikhet.

Formella metoder för korrekthetsverifiering av mjukvara är ett alternativ (eller komplement) till granskning och testning. Området innehåller en omfattande mängd metoder av mycket olika typ, men gemensamt är att egenskaper hos mjukvaran bevisas matematiskt – oftast med hjälp av verktyg i form av datorprogram. De formella metoderna utgår från mjukvaran och antaganden om indata och bevisar egenskaper hos mjukvarans beteende och/eller utdata. Nedan följer två exempel på användning av formella metoder.

1. En programfunktion tar ett antal argument i form av flyttal och gör sedan en lång rad komplicerade beräkningar med dessa och returnerar ett svar i form av ett flyttal. Utvecklarna vill vara säkra på att beräkningarna aldrig resulterar i en over-/underflow eller en division med noll. Med rätt verktyg går det att verifiera att detta aldrig händer, givet att indata håller sig inom vissa givna gränser.
2. En programfunktion tar en array av heltal som indata och ska returnera dessa heltal i en ny array, sorterad från minsta till största heltal. Genom att definiera de önskade egenskaperna i en formell notation går det att verifiera att källkoden implementerar ett program som resulterar i dessa egenskaper.

[1] Se publikationslista i kapitel 7

I det första exemplet verifierades en egenskap på låg nivå, nämligen avsaknaden av några typer av specifika beräkningsfel. I det andra fallet verifierades den logiska korrektheten hos en viss programfunktion. Detta gjordes genom att beskriva programfunktionen i en formell notation och visa att programkoden var logiskt ekvivalent med denna. De två exemplen visar på spännvidden hos det som går under samlingsbegreppet formella metoder. I ena änden finns metoder och verktyg för att leta efter (eller utesluta) vanliga typer av fel. I andra änden finns metoder och verktyg som omfattar hela utvecklingsprocessen, som använder abstrakta beskrivningar av önskad funktionalitet som referenspunkt. Sedan går det att antingen (via flera delsteg) generera garanterat ekvivalent programkod, eller bara visa att en föreslagen programkod är ekvivalent med den abstrakta beskrivningen.

2.2.1 Formella metoder år 1

Under projektets första år gjordes en översikt över vad som går att uppnå med formella metoder och vilka begränsningar som finns, vilka huvudsakliga metoder som finns och vilka akademiska forskningsgrupper i Sverige som forskar inom området. Projektet genomfördes huvudsakligen i form av litteraturstudier, kompletterat med ett antal intervjuer med forskare inom området. Resultatet av studien redovisades i rapporten *Overview of formal methods in software engineering*. I rapporten presenteras en kortfattad introduktion till forskningen om formella metoder tillsammans med en klassificering av olika, existerande formella metoder. Ett urval av forskningslitteraturen inom området presenterades och några system beskrevs där formella metoder använts för att bevisa säkerhetsegenskaper. Slutsatsen som drogs var att det finns formella metoder som fungerar och att det kan vara kostnadseffektivs och tidseffektivt att använda dem. Av denna anledning bedömdes området vara intressant för Försvarsmaktens behov.

2.2.2 Formella metoder år 2

Under projektets andra år fokuserades projektet på en specifik typ av formella metoder, så kallad *white-box fuzzing*. White-box fuzzing kan ses som ett sätt att skapa testdata som på ett effektivt sätt triggar fel som finns i det program som ska verifieras. En (automatisk) *symbolisk analys* av programkoden genererar testfall utifrån vilka datarelationer som är kända för att kunna orsaka problem. Om något av dessa testfall får programmet att bryta mot sin specifikation framgår inte bara att programmet innehåller en viss typ av fel, det resulterar dessutom i ett explicit exempel på när felet dyker upp.

White-box fuzzing är inte ett sätt att bevisa att program är korrekta, utan ett sätt, baserat på formell analys, att hitta fel i programkod. Metoden som sådan har dock visat sig vara effektiv, t.ex. använder Microsoft kontinuerligt en egen implementation av white-box fuzzing för att hitta fel i sina produkter under utvecklingsfasen.

Resultaten av studien redovisades i rapporten *White-box fuzzing*. I rapporten beskrevs white-box fuzzing och sattes i relation till andra, besläktade metoder. Vidare listades ett antal verktyg för white-box fuzzing och dessa beskrevs översiktligt. Slutligen presenterades resultatet av en fallstudie där en erfaren systemutvecklare fick prova ett specifikt verktyg, *IntelliTest*, som är en del av Microsoft Visual Studio. Fallstudien gav ett positivt utfall på flera sätt: användandet av IntelliTest tog inte särskilt mycket tid, flera buggar hittades som utvecklaren själv missat och användarupplevelsen var positiv.

2.2.3 Formella metoder år 3

Under projektets tredje år gjordes en verklighetsliknande analys av ett datorprogram, liknande det arbete som kan ligga till grund för någon form av certifiering. Syftet med analysen var att identifiera vilka programegenskaper som är särskilt viktiga att verifiera och i vilken utsträckning det finns verktyg som kan stödja med detta.

Datorprogrammet som valdes ut för analys var *OpenVPN*[2] med *mbed TLS*[3] som underliggande kryptobibliotek. Dessa ansågs vara representativa för en typ av programkod som Försvarsmakten använder sig av i vissa av sina IT-system. OpenVPN och mbed TLS har flera egenskaper som gör koden lämplig att utvärdera formella metoder på: all källkod finns tillgänglig, de är skrivna helt i C – vilket är typiskt för denna typ av program, de är av en hanterlig storlek, har relativt låg komplexitet och koden är välskriven.

Inledningsvis formulerades några övergripande säkerhetsmål som behövde verifieras. Dessa bröts ned och tolkades i flera steg tills dess att de kunde formuleras som egenskaper hos programkoden. Några egenskaper valdes ut för formell verifiering och lämpliga verktyg identifierades och användes. En fullständig verifiering av den säkerhetsmässiga korrektheten hos hela OpenVPN och mbed TLS har inte varit syftet, varför varken säkerhetsmålen eller programkodsegenskaperna som valdes ut för verifiering var fullständiga, utan de valdes istället för att vara representativa.

Med detta som bakgrund genomfördes prov av verktyg genom att utvalda kodegenskaper verifierades formellt. På detta sätt kunde verktyg med relevanta förmågor undersökas och relevanta verktygsegenskaper dokumenteras.

Resultatet av studien kommer inte att finnas tillgängligt förrän efter det att denna slutrapport är färdigställd. Resultatet presenteras istället i en rapport som blir tillgänglig i början av 2018.

2.3 Erfarenheter från utveckling och förvaltning av IT-system

Informationssäkerhet kan upplevas som ett hinder vid utveckling och förvaltning av IT-system, speciellt när det gäller system med höga säkerhetskrav. Detta beror i hög grad på att de säkerhetsåtgärder som behövs för ett sådant system medför ett omfattande arbete innan ett system är ackrediterat och får användas i verksamheten.

I detta arbete genomfördes en intervjustudie avseende erfarenheter av säkerhetsarbete relaterat till IT-system för hantering av information som omfattas av försvarssekretess. Respondenterna arbetade med frågor relaterade till IT-säkerhet hos Försvarsmakten, civila myndigheter och näringslivet. Deras samlade erfarenhet omfattade teknik och processer under utveckling, ackreditering och drift.

Resultatet av studien redovisades i rapporten *Erfarenheter från utveckling och förvaltning av IT-system*. Rapporten beskriver hur respondenterna gav en bild av att det finns många utmaningar i strävan mot det ideala men ouppnåeliga målet med absolut säkerhet. Systemen ökar i komplexitet, vilket gör ackrediteringsprocessen allt mer krävande. Dessutom ökar kommunikationen mellan IT-system vilket ger högre exponering mot angrepp. Ett överdrivet fokus på säkerhet kan leda till system som kräver mer tid och pengar att ta fram, samtidigt som nya arkitekturer och funktioner uteblir. Respondenterna var i stora drag överens om att det nuvarande tankesättet behöver justeras så att fokus hamnar på ett kontinuerligt och aktivt säkerhetsarbete under hela systemets livslängd, med en utvidgning från enbart teknisk säkerhet. En viss förändring av synen på risk har redan introducerats i Försvarsmakten men fortfarande verkar yttranden om säkerhet tolkas absolut utan att väga in verksamhetsnyttan.

En slutsats i studien var att det skulle vara värdefullt att utreda hur IT-säkerhetsaspekter och ackreditering ska hanteras i Försvarsmakten för att bättre kunna tillgodose verksamhetens behov i framtiden.

[2] https://openvpen.net
[3] https://tls.mbed.org

2.4 Risker med virtualisering av IT-system

Virtualisering av IT-system är en beprövad och utbredd teknik för att bygga såväl stora datacenterlösningar som mindre installationer. Virtualisering ger ett antal fördelar för drift och verksamhet, men innebär även risker. Denna studie undersökte virtualisering av IT-system med fokus på de risker och sårbarheter som kan uppstå i virtualiserade miljöer. Studien baserades på en litteraturstudie avseende sårbarheter i virtualiseringsmjukvara. Målet med studien var att bidra till förståelsen för de risker som virtualisering innebär, genom att beskriva rapporterade sårbarheter i etablerade virtualiseringsmjukvaror.

Resultatet av studien redovisades i rapporten *Risker med virtualisering av IT-system* och tog främst upp så kallad systemvirtualisering, det vill säga system där den virtualiserade miljön motsvarar en fysisk dator. I rapporten beskrivs hur virtualiserade miljöer i regel innehåller samtliga sårbarheter som finns i motsvarande fysiska miljöer. Virtualisering innebär dessutom att mjukvara tillförs i systemet för att skapa virtualiseringsmiljön, upprätthålla separation och ge ett lämpligt ”hårdvarulikt” gränssnitt mot de virtuella maskinerna. Den tillförda mjukvaran kan innehålla sårbarheter vilket ger ytterligare möjligheter för angripare. Jämfört med fysisk separation finns exempelvis ökad risk för läckage mellan virtuella maskiner och att virtuella maskiner påverkar varandra på oönskade sätt.

Risken för att lyckade angrepp ska få mer utbredda konsekvenser är i regel större i virtualiserade miljöer än i miljöer byggda på fysiskt åtskilda maskiner. I vissa fall är risken acceptabel utifrån de fördelar som virtualiseringen innebär. I andra fall, till exempel om separationen måste skydda information med hög informationssäkerhetsklass, så är risken allt för hög med existerade virtualiseringstekniker. Införandet av virtualisering i ett känsligt IT-system måste därmed föregås av noggranna riskbedömningar för att säkerställa att en tillräckligt låg risknivå upprätthålls.

3 Omvärldsstudier

I detta kapitel beskrivs de omvärldsstudier som genomförts inom ramen för projektet. I kapitel 7 finns fullständiga referenser för de publikationer som hänvisas till i den löpande texten nedan.

3.1 IT-säkerhets- och informationssäkerhets-utbildningar i Sverige

IT-säkerhet och informationssäkerhet är akademiska discipliner med utbildningar i hela spannet från grundnivå till forskarutbildning. Personerna som genomgår dessa utbildningar representerar en stor del av den tillgängliga kompetensen inom dessa områden och utgör därmed en viktig del av rekryteringsunderlaget för kvalificerade tjänster inom Försvarsmakten och andra myndigheter. Denna omvärldsstudie kartlade utbudet av utbildningar på universitetsnivå inom IT-säkerhet och informationssäkerhet.

Resultatet av studien redovisades i rapporten *IT-säkerhets- och informationssäkerhets-utbildningar i Sverige*. Kartläggningen av grundutbildningen inom området redovisade ett antal identifierade utbildningsprogram, inriktningar och påbyggnadsutbildningar. Kartläggningen av forskarutbildningen inom området redovisade antalet producerade licentiat- och doktorsavhandlingar i Sverige mellan 2010 och mitten av 2016.

3.2 Informationssäkerhetsegenskaper – Avvägningar och prioriteringar

Informationssäkerhetsegenskapen *sekretess* har en framträdande roll inom Försvarsmakten, medan egenskaperna *riktighet* och *tillgänglighet* inte har getts motsvarande utrymme. Behov av att beakta riktighet och tillgänglighet lyfts återkommande, men sekretessens framträdande roll är tydlig.

Resultatet i studien redovisades i rapporten *Informationssäkerhetsegenskaper – Avvägningar och prioriteringar*. Studien identifierade övergripande och bakomliggande prioriteringar för att beskriva hur andra informationssäkerhetsegenskaper än sekretess ges utrymme och hanteras inom Försvarsmakten. Syftet var att därigenom påvisa möjliga avvägningar för att nå bästa möjliga balans mellan informationssäkerhetsegenskaperna.

Studiens slutsats var att sammanvägning av olika behovsbilder inom Försvarsmaktens verksamhetsplanering respektive operativa verksamhet har potential att ge bättre balans mellan sekretess, riktighet och tillgänglighet. Riktighets- och tillgänglighetsaspekterna bör ge tydligare avtryck i Försvarsmaktens centrala, styrande dokument. Tydliga analyser som åskådliggör både nyttan och riskerna med ett informationssystem möjliggör avvägningar för att nå bästa möjliga balans mellan alla informationssäkerhetsegenskaperna.

3.3 Regelverksanalys

Försvarsmakten har ett omfattande stöd i författningar, bestämmelser, regelverk och handböcker avseende hur arbete med informationssäkerhet ska bedrivas för att uppnå den säkerhet som krävs för att riskerna för verksamheten ska vara acceptabla. Studiens mål var att göra en sammanställning av vilka dokument som är relevanta i sammanhanget, och deras inbördes relationer. Fokus i studien var att beskriva de dokument som är relevanta för ett IT-systems säkerhet under utvecklingsfasen fram till ackrediteringsbeslut.

3.4 Objektbaserad säkerhet

Objektbaserad säkerhet är en vision om säkerhetslösningar där informationsobjekt själva kan upprätthålla en skyddsnivå enligt en given policy samt hantera åtkomst till informationen bortom informationsägarens egna system. Med objektbaserad säkerhet kan en informationsägare distribuera informationsobjekt, exempelvis en pdf-fil, över osäkra kanaler och till icke identifierade men behöriga mottagare, utan att en obehörig aktör kan tillgodogöra sig eller påverka innehållet i informationsobjektet. Ett informationsobjekt skyddat genom objektbaserad säkerhet ska således skydda innehållet mot exponering samtidigt som en policybaserad åtkomstkontroll efterlevs.

Arbetet med objektbaserad säkerhet startade i FoT-projekten *Objekt och tjänstebaserad säkerhet* samt *Objektbaserad säkerhet* och har fortsatt som en del av projektet Teknik för IT-säkerhet. Inom projektet Teknik för IT-säkerhet har den akademiska utvecklingen av tekniker för objektbaserad säkerhet följts under projektets samtliga tre år.

3.4.1 Objektbaserad säkerhet år 1

Under det första året följdes utvecklingen inom området attributbaserad kryptering genom en litteraturstudie som redovisades i memot *Objektbaserad säkerhet – omvärldsbevakning av attributbaserad kryptering*. Studien syftade dels till att identifiera aktuella trender, dels till att hitta artiklar med militär anknytning vad gäller innehåll eller finansiering.

De vanligaste frågeställningarna bland publicerade studier under året handlade om molntjänster och personlig integritet. Tillämpningar i den traditionellt militära domänen hade studerats bland annat inom försvarsalliansen Nato, främst genom *NATO Communication & Information Agencys* (NCIA) arbete med åtkomstkontroll. Den lösning som beskrivs var ett åtkomstsystem som skiljer på frågorna ”Vad får släppas ut?” och ”Hur förvarar vi aktuell fil?”. NCIA:s lösning kallas för *Content Protection and Release* (CPR) och baserades på attributbaserad åtkomstkontroll. Genom att kombinera tekniker för attributbaserad åtkomstkontroll med tekniker för objektbaserad säkerhet (Object Level Protection, OLP) uppvisar NCIA ett system där det är möjligt att automatiskt dela information med koalitionspartners baserat på vilka de är (behörighet) samt deras förmåga att hantera informationen (resursen) i sina system (miljö). En automatiserad åtkomstkontroll leder till ett snabbare och mer konsekvent hanterande av information.

3.4.2 Objektbaserad säkerhet år 2

Under andra året presenterades i memot *Objektbaserad säkerhet* en översikt över forskningsläget avseende tekniker och tillämpningar för tekniker som kan användas för objektbaserad säkerhet. De tekniker som togs upp var attributbaserad åtkomstkontroll och attributbaserad kryptering. De tillämpningar av tekniker som identifierades var digitala patientjournaler, automatiserad och policybaserad åtkomstkontroll samt attributbaserad kryptering i robusta nätverk.

En slutsats som drogs i omvärldsstudien var att det fanns ett tydligt önskemål inom militära tillämpningar, främst inom Nato, att gå mot ett mer automatiserat stöd för åtkomstbeslut mellan koalitionspartners. Arbetet med att låta ett åtkomstsystem tolka en policy hade pågått i flera år och hade ett tydligt tillämpningsområde inom *Federated Mission Networking*.

3.4.3 Objektbaserad säkerhet år 3

Även under projektets sista år genomfördes en omvärldsbevakning av akademiska publiceringar av tekniker som kan användas för objektbaserad säkerhet. Antalet årligt publicerade artiklar har ökat något över den senaste treårsperioden men jämfört med attributbaserad kryptering är attributbaserad åtkomstkontroll ett ganska litet

forskningsområde. Attributbaserad åtkomstkontroll är å andra sidan tillämpat som lösning i flera artiklar.

Både attributbaserad kryptering och attributbaserad åtkomstkontroll är intressanta lösningar för åtkomstkontroll för digitaliserade lösningar såsom mobila plattformar och Sakernas internet. I dessa miljöer behöver information kunna röra sig mer över olika plattformar och mottagaren (konsumenten) behöver inte vara en person.

4 Seminarieverksamhet

FOI har i flera år genomfört en seminariedag där de viktigaste resultaten från FOI:s FoT-projekt inom området informationssäkerhet har presenterats för intresserade inom FM och FMV.

År 2015 övertogs seminarieverksamheten av FoT-projektet *Teknik för IT-säkerhet*. I samband med detta breddades upplägget så att FOI, FM och FMV alla deltog med presentationer. I samband med detta ändrades namnet till IT-säkerhetsdagen och inbjudan skickades till en bredare krets. Samordningen med FM och FMV gjorde också att IT-säkerhetsdagen och FMV:s informationsinfrastrukturdag, ett evenemang med ungefär samma målgrupp, kunde läggas dagarna efter varandra i samma lokal. Resultatet för IT-säkerhetsdagen blev mycket lyckat och antalet deltagare var fler än 100 – mer än dubbelt så många som 2014 och ungefär fyra gånger så många som före 2014.

År 2016 samordnades IT-säkerhetsdagen och informationsinfrastrukturdagen både vad gäller planering och genomförande. De två evenemangen erbjöd presentationer från FOI, FM, FMV, FRA och MSB. Öppningsanförandet hölls av LEDS CIO, generalmajor Fredrik Robertsson. Antalet deltagare var drygt 200 personer.

År 2017 byttes namnet till IT-försvarsdagen för att tydligare skilja sig från andra IT-säkerhetsdagar. Presentationer hölls av FOI, FM, FMV, FRA och MSB. Antalet deltagare var cirka 250 personer och ytterligare ungefär 70 önskade delta men kunde inte beredas plats.

Baserat på det stora intresset och den återkoppling som kommit är vår uppfattning att seminarieverksamheten i form av IT-säkerhetsdagar/IT-försvarsdag varit värdefull. Verksamheten kommer att fortsättas inom ramen för kommande FoT-projekt.

5 Arbete i Natogruppen IST-114

Inom FoT-projektet *Objektbaserad säkerhet* som avslutades 2014 deltog en FOI-medarbetare i Natoforskningsprojektet *Trusted information sharing for partnership* (IST-114). Syftet med deltagandet var att arbeta med frågan huruvida egenskaperna riktighet och tillgänglighet kan utvecklas och bli kriterier för åtkomstbeslut. Om riktighet och tillgänglighet kan beskrivas med samma tydlighet som sekretess, skulle en policy kunna styra över situationer där sekretess inte är aktuellt alternativt inom en informations-säkerhetsklass. Möjligheten att beskriva riktighet och tillgänglighet är intressant både för attributbaserad åtkomstkontroll och attributbaserad kryptering.

Ett avslutande möte återstod efter 2014 och det genomfördes inom ramen för projektet Teknik för IT-säkerhet. Slutsatserna från arbetet är att det går att bedöma riktighet och tillgänglighet på samma sätt som Försvarsmaktens informationssäkerhetsklasser, det vill säga i en skala baserad på konsekvens av ej uppnådd eller komprometterad egenskap. Svårigheten med arbetet var att identifiera relevanta konsekvenser. Arbetet utmynnade i den vetenskapliga publikationen *Labelling for Integrity and Availability*[4].

[4] Se fullständig referens i kapitel 7.

6 Projektet som helhet

I redovisningen i kapitlen 2 till 5 framgår projektets verksamhet och resultat under de tre projektåren. Nedan visas hur de olika projektverksamheterna förhåller sig till de områden som pekas ut i FoT-planens beskrivning.

De områden (inklusive projektets frågeställningar) som FoT-planen pekar ut är:

(1) Vilka IT-säkerhetstekniker och -metoder finns som kan användas för att inom Försvarsmakten möjliggöra effektiv IT-användning med bibehållen IT-säkerhet?

(2) Vilka IT-säkerhetstekniker och -metoder finns som kan möjliggöra användning av icke-militära informationssystem för militärt bruk?

(3) Hur kan identifierade IT-säkerhetstekniker enligt ovan nyttjas inom Försvarsmakten?

(4) Omvärldsanalys som ger en övergripande bild av vilka IT-säkerhetstekniska frågor som är aktuella i Försvarsmakten samt vilken forskning som bedrivs i landet.

(5) Formella metoder ska studeras och bevakning av objektbaserad säkerhet ska göras.

Tabell 1: Projektverksamheternas koppling till de områden FoT-planen pekar ut.

	Område i FoT-planen				
Projektverksamhet	**1**	**2**	**3**	**4**	**5**
Verktyg för att åstadkomma pålitlig programvara	X	X			
Formella metoder	X	X	X		X
Erfarenheter från utveckling och förvaltning av IT-system	X			X	
Risker med virtualisering av IT-system	X	X	X	X	
IT-säkerhets- och informationssäkerhetsutbildningar i Sverige				X	
Informationssäkerhetsegenskaper – Avvägningar och prioriteringar				X	
Regelverksanalys				X	
Objektbaserad säkerhet	X		X	X	X
Seminarieverksamhet				X	

Seminarieverksamheten kan synas vara svår att passa in bland de givna områdena för projektets verksamhet. Det finns dock ett tydligt omvärldsbevakande innehåll i denna verksamhet, dels genom de presentationer som görs av personer utanför FOI, dels i den mycket stora kontaktyta som uppstår i samband med dessa seminarier. Om det dessutom uppfattas som rimligt att projektverksamheten kan ha inslag av annat än studier, så kan de kontakter som uppstår i seminarieverksamheten ses ge värdefull input och återkoppling till alla projektets delar. Seminarieverksamheten fungerar också som kommunikationskanal från FOI:s projektverksamhet till framför allt Försvarsmakten och Försvarets Materielverk. Detta gynnar inte bara projektet Teknik för IT-säkerhet utan även andra projekt inom informationssäkerhetsområdet.

Projektets utgångspunkt har varit teknisk och projektmedlemmarnas intresseområde är väsentligen teknik. Trots detta har projektaktiviteterna ofta lett vidare till icke-tekniska frågeställningar, såsom regelverk, organisation och processer. Ett exempel på detta är studien *Erfarenheter från utveckling och förvaltning av IT-system*, som tydligt fokuserar på andra faktorer än teknik, men som är både relevant och intressant. I projektet ser vi det som en effekt av att det är svårt att frikoppla tekniken från sin kontext, vilket ger denna effekt när forskningen tillåts följa de trådar som syns vara mest värdefulla. Vi ser det som en stor fördel att kunna välja det fokus som bedöms ge mest relevanta resultat och störst effekt för Försvarsmakten inom det studerade området.

7 Publikationslista

Inom projektets ram har följande publikationer producerats:

Rapporter

I. Rodhe och M. Karresand, *Overview of formal methods in software engineering*, FOI-R--4156--SE, 2015.

A. Hunstad och I. Rodhe, *IT-säkerhets- och informationssäkerhetsutbildningar i Sverige*, FOI-R--4160--SE, 2015.

I. Rodhe och M. Karresand, *Verktyg för att åstadkomma pålitlig programvara*, FOI-R--4290--SE, 2016.

M. Cohen, I. Rodhe och J. Löfvenberg, *White-box fuzzing*, FOI-R--4329--SE, 2016.

A. Gudmundson Hunstad, *Informationssäkerhetsegenskaper – Avvägningar och prioriteringar*, FOI-R--4341--SE, 2016.

H. Karlzén, D. Eidenskog och J. Löfvenberg, *Erfarenheter från utveckling och förvaltning av IT-system*, FOI-R--4423--SE, 2017.

D. Eidenskog och M. Karresand, *Risker med virtualisering av IT-system*, FOI-R--4448--SE, 2017.

J. Löfvenberg, Teknik för IT-säkerhet – Slutrapport, FOI-R--4496--SE, 2017.

A. Gudmundson Hunstad, Rutiner och regelverk för att godkänna IT-system i Försvarsmakten, FOI-R--4526--SE, 2017.

Rapporter med preliminära titlar

C. Bildsten, M. Cohen, D. Eidenskog, J. Löfvenberg, Verktyg för formell verifiering av säkerhetsfunktioner i mjukvara, 2017. (ännu inte tillgänglig)

Memon

L. Westerdahl, *Objektbaserad säkerhet – omvärldsbevakning av attributbaserad kryptering*, FOI Memo 5512, 2015.

J. Löfvenberg, *IT-säkerhetsdagen 2015*, FOI Memo 5614, 2016.

J. Löfvenberg, *IT-säkerhetsdagen 2016*, FOI Memo 5847, 2016.

J. Löfvenberg, *IT-försvarsdagen 2017*, FOI Memo 6219, 2017.

L. Westerdahl, *Objektbaserad säkerhet*, FOI Memo 5859, 2016.

L. Westerdahl, *Trender inom Objektbaserad säkerhet*, FOI Memo 6273, 2017.

Vetenskapliga publikationer

J. Melrose, K. Wrona, T. Guenther, R. Haakseth, N. Nordbotten och L. Westerdahl, ”Labelling for integrity and availability”, *2016 International Conference on Military Communications and Information Systems (ICMCIS)*, 2016, ss. 1–8.

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