LINDHOLMEN SCIENCE PARK

SECURITY ARENA

Utveckling för säker krishantering

ÅRSRAPPORT 2009

Projektledningsgrupp Security Arena

Bo Norrhem
Programchef
Security Arena

Mikael Lagerman
Projektledare Tema 2
Ericsson

Erland Jonsson
Projektledare Tema 4
Chalmers

Mikael Korhonen
Koordinator
Koncept och förmågeutveckling
MSB

Mikael Fredin
Projektledare Tema 3
Saab AB

Torbjörn Andreasson
Projektledare Tema 2
Ericsson

Leif Axelsson
Projektledare Tema 1
Volvo

Viveca Norén
Forskningssamordnare
MSB

Innehållsförteckning

Förord och läsanvisningar

Denna årsrapport beskriver det arbete som utförts under 2009 på Security Arena. Den har föregåtts av liknande årsvisa rapporter sedan Security Arenas start 2005. Syftet med rapporten är att lämna en redogörelse för den verksamhet som bedrivits och att särskilt belysa de resultat som bedöms som mest intressanta för Myndigheten för samhällsskydd och beredskap (MSB) och andra intressenter.

För att underlätta läsningen av rapporten följer här några läsanvisningar:

- Rapporten innehåller två huvudkapitel: *Generella resultat uppnådda under 2009* och *Specifika resultat inom forskning och utveckling*. Det förra beskriver samordning och samverkansaktiviteter, konferenser och seminarier m.m., medan det senare beskriver genomfört utvecklingsarbete och pågående forskning inom ett antal definierade områden. För varje område ges en kort sammanställning av uppnådda resultat 2009 samt vilken inriktning på arbetet som planeras för 2010.

- Resultat från enskilda projekt återfinns under respektive temaområdesbeskrivning.

- Alla förkortningar och begrepp förklaras i en lista sist i rapporten.

- Dokumentet har fem bilagor.

Sammanfattning

För beskrivning av Security Arenas övergripande verksamhet och organisation, samt definitioner av ett antal begrepp, se kapitlet *Lindholmen Science Park driver samverkansprogrammet Security Arena*.

Inriktning på forskning och utveckling på Security Arena 2009

Under 2009 har forskning och utvecklingsarbete i huvudsak bedrivits enligt gällande avtal mellan Lindholmen Science Park och Myndigheten för samhällsskydd och beredskap (MSB). Konceptgenerering, pilotprojekt och studieuppdrag har både bedrivits inom de definierade temaområdena samt i ett fristående uppdrag, men också i ett par nyutvecklade samarbetsprojekt som en spin-off till den avtalsreglerade verksamheten.

Fokus inom temaprojekten har i år legat på teknik för avancerad områdesövervakning, informationshantering och hot från organiserad brottslighet mot transportsektorn.

Det har skett en fortsatt utveckling av Security Arenas arbetsmodell med tidig användarmedverkan i forskning och konceptgenerering. Via behovsanalyser med aktiv medverkan från områdes-experter visar arbetsresultaten att det går att utveckla relevanta koncept som i ett nästa steg leder till praktiska prov tillsammans med användargrupper.

En förstudie med MSBs lägescentral har genomförts i syfte att hitta tänkbara projekt som kan utveckla nya förmågor hos lägescentralen. Detta arbete kommer att fortsätta under 2010.

Samordning och samverkan

Security Arena har följande huvudaktörer: MSB, Chalmers tekniska högskola, Göteborgs universitet, Ericsson, Saab AB, AB Volvo. Dessutom medverkar slutanvändare, expertgrupper och samverkanspartners.

Flera nya samarbeten som initierades under 2008 har vidareutvecklats under 2009. Bland annat har kontakterna med Umeå universitet resulterat i ett konkret projektsamarbete mellan Security Arena och CBRNE-centret inom EU/FP7. Dessutom har projektsamverkan med SAFER och Viktoriainstitutet fördjupats tack vare satsningarna på forskningsprojektet LiveResponse™ med Viktoriainstitutet som utförare. Förutom fortsatt och utökad samverkan med nya instanser inom MSB har också samarbete med ett antal nya europeiska potentiella samverkansparter utvecklats.

Kunskapsutveckling och informationsspridning

Informationsspridningen har skett genom deltagande i en mängd konferenser och seminarier både nationellt och internationellt. På det lokala planet har lunchseminarieserien fortsatt att utvecklas under året och når idag en bredare målgrupp än tidigare. Ämnesområdena för seminarierna har också utökats, vilket gör att vi når fler intressenter. Specifikt mot MSB kan nämnas att förstudien med MSBs lägescentral har gett möjlighet för Security Arenas parter att presentera en mängd resultat från genomfört arbete.

Utvärdering och nytt ramavtal

Under året genomfördes en utvärdering av det arbete som bedrivits på Security Arena från 2005. Utvärderingen var intervjubaserad och utfördes av Faugert & Co på uppdrag av MSB. Ett drygt 20-tal intressenter intervjuades och fick delge sina erfarenheter och synpunkter. Utvärderingen visade bl.a. på att samverkan mellan inblandade aktörer fungerar väl och att samarbetet ger tillgång till kontakter, information och problemställningar även utanför det egna området. En viktig styrka som framhölls var överensstämmelsen mellan hur satsningen är tänkt att fungera, dess programlogik, samt hur parterna de facto uppfattar verksamheten.

I samband med 2009 års utgång upphörde det gällande ramavtalet mellan MSB och Lindholmen Science Park. Ett nytt ramavtal för perioden 2010 till och med 2012 har tecknats.

Inriktning 2010

Planeringen av 2010 års arbete och framåt ska göras under våren. Fokus kommer att ligga på att ytterligare förstärka förmågan till behovsanalyser och innovativa lösningar i genereringen av koncept samt att knyta fler forskarkontakter med pågående samhällssäkerhetsforskning såväl nationellt som internationellt. Inriktningen är att de tematiska områdena ska bibehållas, men en värdering och omprövning kommer att ske. Detta kan resultera i någon eller några förändringar framöver.

Lindholmen Science Park driver samverkansprogrammet Security Arena

Lindholmen Science Park är ett geografiskt kluster i Göteborg och ett forskningscenter där flera stora projektplattformar drivs med bas på Lindholmen. Bolaget arbetar med att stimulera och organisera nya former av samverkan mellan näringsliv, högskola och samhälle där inriktning sker mot följande tre fokusområden:

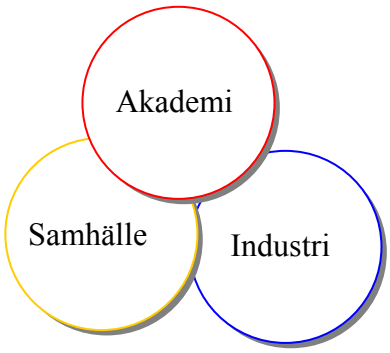
- Mobilt Internet
- Intelligenta fordon och transportsystem
- Modern media och design

Dessa områden engagerar ett stort antal personer och aktiviteter. Forskning och utveckling inom samhällssäkerhetsområdet omfattar i olika grader dessa fokusområden. Projekten och uppdragen som drivs inom Lindholmen Science Park kännetecknas av gränsöverskridande samarbete, både gällande kompetens, organisation och mellan olika länder. Flera av de test- och utvecklingsmiljöer som drivs inom Lindholmen Science Park har resulterat i gemensamma internationella standarder.

Det övergripande målet är att fortsätta utveckla Lindholmen Science Park till ett världsledande forskningscenter för ny teknologi och kommunikation.

Verksamheten på Security Arena

Sedan 2005 driver Lindholmen Science Park Security Arena som är ett forsknings- och utvecklingsarbete i samverkan mellan huvudaktörerna MSB, Chalmers tekniska högskola, Göteborgs universitet, AB Volvo, Saab AB och Ericsson. Samarbetet bedrivs enligt den s.k. Triple Helix-modellen, det vill säga i samverkan mellan samhälle, akademi och näringsliv.



Verksamheten bedrevs under de första åren i form av årsvisa uppdrag och under perioden 2007-2009 inom ramen av ett treårigt avtal. På uppdrag av MSB utförde Faugert & Co under hösten 2009 en intervjubaserad utvärdering av genomfört arbete.[1] Som styrkor framhölls bl.a. den öppna och neutrala mötesplatsen, att samverkan mellan aktörer fungerar bra, att frågeställningarna är både relevanta och användarnära samt att verksamhetens fokus överensstämmer väl med programmets övergripande mål. Bland förbättringsutrymmen kan nämnas bättre omhändertagande av resultat och synergimöjligheter, smidigare finansieringsformer för projekten samt en önskvärd breddning av akademisk kompetens.

Ett nytt ramavtal för fortsatt forskning och utveckling inom Security Arena under perioden 2010-2012 har tecknats mellan Lindholmen Science Park och MSB. Det liknar till stor del det tidigare ramavtalet. Verksamhetens nya målsättningar, arbetsformer och organisation beskrivs i en verksamhetsplan som färdigställs under första kvartalet 2010.

Det övergripande syftet med arbetet inom Security Arena är att bedriva forskning, teknik- och metodutveckling som bidrar till att stärka samhällets förmåga att hantera kriser och olyckor. Arbetet karakteriseras av samverkan med ett stort engagemang från olika områdesexperter, bl.a. från olika universitet och högskolor, myndigheter, kommuner och företag med flera.

Ett antal temaområden har definierats och inom varje temaområde genomförs olika delprojekt av företrädesvis teknisk karaktär. Inom några av delprojekten bedrivs rent forskningsarbete som därför av naturliga skäl har en särskild karaktär. Förutom temaområdena genomförs seminarieverksamhet, workshops och olika studieuppdrag i samverkan mellan industriparterna och akademi.

Under 2009 bedrevs arbete på Security Arena inom följande fyra temaområden:

- Tema 1: Samhällskritiska transporter - forskning och utveckling av säkrare försörjningskedjor, förmågan att bemöta hot från organiserad brottslighet, transporter av farligt gods och säkrare och effektivare transportflöden genom hamnanläggningar.

[1] Technopolis Group, Utvärdering av Security Arena, 2009-11-13, MSB 2009-2959-11

- Tema 2: Mobilt bredband för säkerhet i samhället - forskning och utveckling av hur kommersiella kommunikationsteknologier kan ge myndighetsanvändare bättre stöd för informationsdelning i krissituationer.

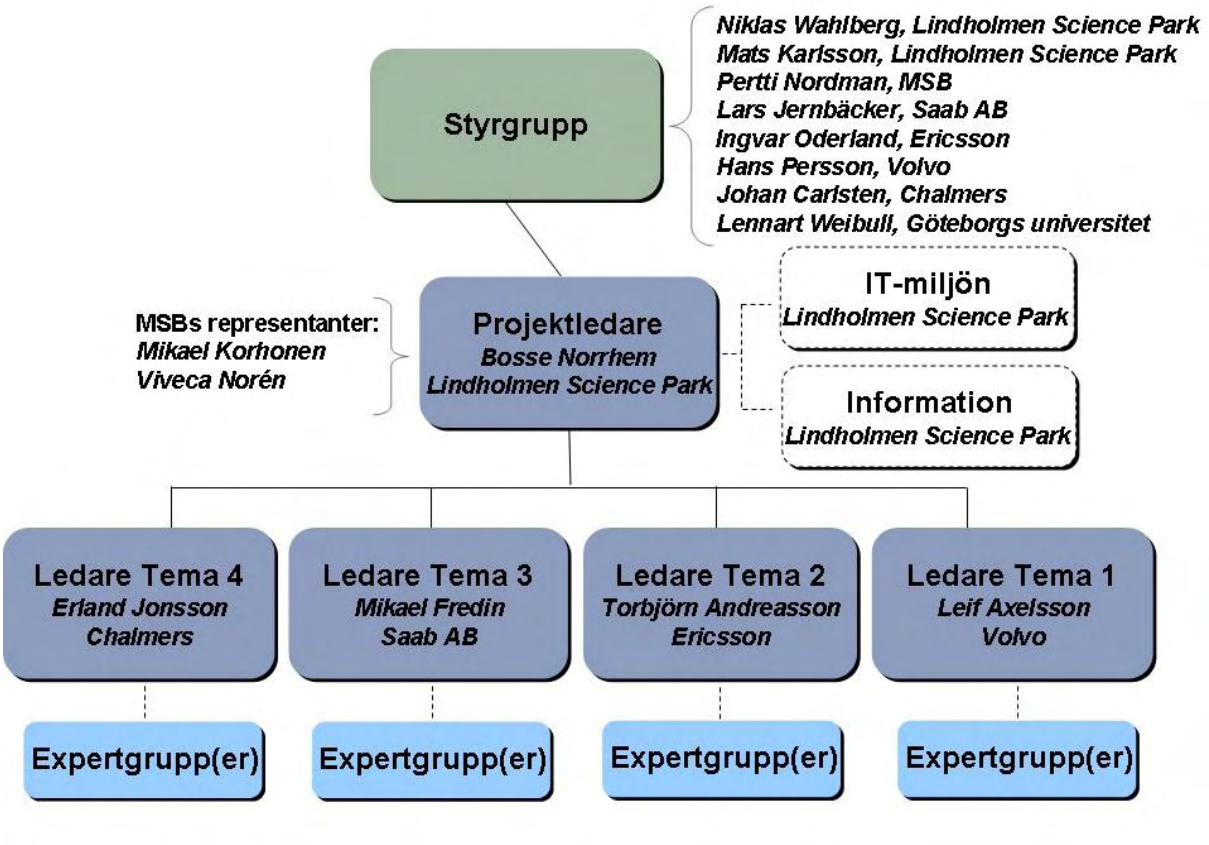
- Tema 3: Surveillance and Early Warning - forskning och utveckling av teknik för övervakning av samhällskritiska infrastrukturer, i syfte att så tidigt som möjligt ge varning vid risk för eskalerande kriser i samhället. Bidrar aktivt till att höja samhällets krisberedskap genom att studera tekniker och metoder för att stödja samverkan på alla nivåer i krishanteringssystemet.

- Tema 4: Metoder och system för robust och säker krishantering - forskning inom metoder och tekniker för förebyggande krishantering inkluderande data- och informationssäkerhet.

Varje temaområde har etablerat expertgrupper bestående av representanter från olika organisationer i krishanteringssystemet. Experterna bidrar med behovsanalys och problem-formuleringar till stöd för utvecklingen av de olika delprojekten inom respektive temaområde. Expertgrupperna har en avgörande roll som stöd till forskarna och för utvecklingen av koncept och pilotprojekt. De områdesexperter som varit verksamma under 2009 omnämns i Bilaga 2.

Organisation

Arbetet på Security Arena leds av Lindholmen Science Park och har under 2009 varit organiserat på följande sätt:

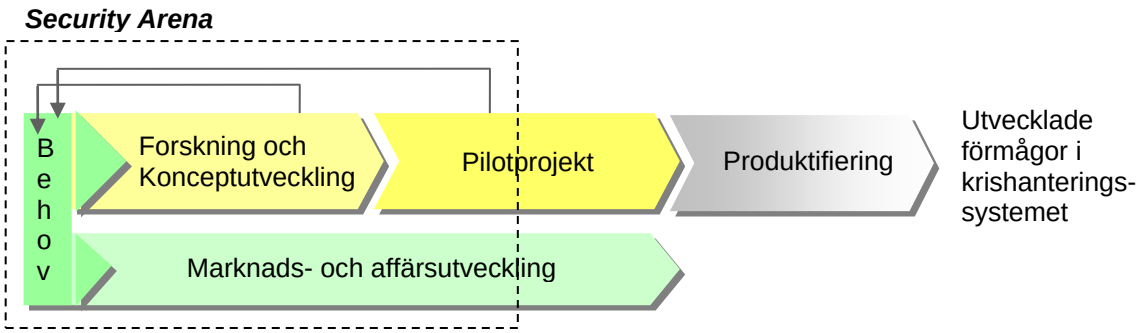


Figur 1. Security Arenas organisation

Arbetsmodell

Security Arenas arbetsmodell är i första hand av konceptuell karaktär med inriktning mot utveckling av framtida nya förmågor inom krishanteringssystemet. I detta ryms även pilotprojektverksamhet där användargrupper kan knytas till arbetet och på lämpliga sätt utvärdera framtagna teknik- och metodkoncept.

Security Arenas roll, sett ur perspektivet av olika utvecklingssteg fram mot nya färdigutvecklade förmågor i krishanteringssystemet, kan illustreras enligt följande:



Figur 2. Utvecklingssteg

Arbetet bedrivs med återkommande behovsanalyser som utgör en grund för både forskningsarbetet, konceptutvecklingen och praktiska prov och försök. Verksamheten resulterar i första hand i s.k. konceptdemonstratorer, pilotprojekt eller forskningsrapporter.

- Med behovsanalys avses att identifiera en eller flera förmågebrister och uttrycka detta i form av en eller flera nya önskvärda behov som en enskild aktör, eller flera aktörer i samverkan, upplever i sin roll och yrkesutövning.

- Med konceptdemonstrator avses en demonstrator som utvecklas för och demonstreras i en rent virtuell miljö. Ett exempel på detta kan vara att påvisa hur en effektivare utnyttjad informationsdelning mellan aktörer kan bidra till en förbättrad lägesuppfattning vilket i sin tur ger ökade förutsättningar till koordinerat beslutsfattande.

- Med pilotprojekt avses prov och försök i en verklig, men inte nödvändigtvis operativ miljö. Detta kan vara insamling av verkliga data för ett speciellt syfte eller att en utsedd användar-grupp utvärderar en ny typ av funktionalitet.

- Med marknadsutveckling avses att analysera förutsättningarna för ett koncept att i ett senare utvecklingssteg kunna nyttiggöras för ingående parter i en operativ miljö. Här har genomförts två uppdrag[2] med analyser på ett generellt plan för samhällssäkerhetsområdet, men det är även relevant att beakta förutsättningarna för hur enskilda koncept kan introduceras på marknaden.

Arbetsmetoden som tillämpas för att utveckla koncept och pilotprojekt är sekventiell och innebär medverkan från områdesexperter från steg 1 enligt:

1. Etablering av expertgrupp med specialistkunskaper inom respektive temaområde och/eller projekt.

---

[2] Security Arena-rapport, Inledande marknadsanalys, 2008-02-01 och Security Arena-rapport, Security Arena marknadsutvecklingsanalys 2008, 2008-12-18, Lindholmen Science Park

2. Behovsanalys som genomförs via intervjuer och workshops med expertgruppen och andra relevanta aktörer.

3. Konceptgenerering baserad på genomförd behovsanalys.

4. Utveckling av konceptdemonstrator.

5. Återkoppling till expertgruppen via demonstration.

6. Utvärdering och eventuell kvalificering för pilotprojekt. Förutom expertgruppens bedömning av konceptets nytta beaktas de tekniska förutsättningarna för ett pilotprojektgenomförande och möjligheten att etablera en relevant användargrupp.

Under 2009 har nedanstående projekt genomförts:

- Fyra projekt inom Tema 1, Samhällskritiska transporter
    - Demoteatern - Säkra transporter
    - Hot från organiserad brottslighet mot transportsektorn
    - International End-to-End (E2E) Transport Security
    - Förstudie: Affärsmodeller för security-tjänster (i samverkan med Tema 2)
- Tre projekt inom Tema 2, Mobilt bredband för säkerhet i samhället
    - Förstudie: Affärsmodeller för security-tjänster (i samverkan med Tema 1)
    - LiveResponse™ (projektet genomfört i samverkan med SAFER och Viktoriainstitutet)
    - Identifiering av behov inom området mobil kommunikation
- Ett projekt bestående av tre delprojekt inom Tema 3, Surveillance and Early Warning
    - Information Flow Management
        - Intelligent Sensor Network
        - Information Management
        - Situation Awareness
- En förstudie med MSBs lägescentral

Tema 4 har genererat ett stort antal vetenskapliga publikationer och examensarbeten. Även andra resultat har synts i form av medverkan vid konferenser och workshops, samverkan med aktörer inom och utom projektet samt informationsspridning.

Uppnådda resultat redovisas per projekt i särskilda kapitel i denna rapport.

GENERELLA RESULTAT UPPNÅDDA UNDER 2009

Generell utveckling av verksamheten

Den generella utvecklingen på Security Arena under 2009 har karakteriserats av ett fortsatt arbete inom definierade temaområden samt ett fördjupat samarbete med ett antal nya samverkansparter.

Tillsammans med SAFER har vi satsat på att utveckla forskningsprojektet LiveResponse™ med Viktoriainstitutet som utförande part. Projektet har bedrivits med medverkan från bl.a. Räddningstjänsten i Stor-Göteborg och Västra Götalandsregionen. Detta har resulterat i en modell för användning av live-video i ett nätverk med ”blåljusaktörer” samt en beskrivning av nyttan av denna teknik ur användarnas perspektiv. Ur projektresultatet har också genererats ny kunskap kring design av system för användargenererat innehåll för blåljusaktörer, något som ligger till grund för nästa steg i projektet som påbörjats under hösten och ska pågå fram till våren 2010. Syftet är då bl.a. att ytterligare förfina tekniken och uppnå bättre kvalitet på bildöverföringen.

Som en ytterligare spin-off från den ordinarie verksamheten har vi under hösten beviljats medel för ett EU FP7-projekt under ledning av Umeå universitet och det s.k. europeiska CBRNE-centret. Projektet ska drivas i samverkan med fjorton europeiska partners med start 2010. Projektet heter CBRNEmap och syftar till att utveckla ett framtida ”system” för skademinimering vid olyckor eller attacker där farliga och explosiva ämnen förekommer. Security Arena kommer att ansvara för specificering av en teknisk demonstrator utifrån identifierade förmågebrister och användarkrav.

Fortsatta satsningar inom EUs forsknings- och utvecklingsprogram har också genomförts dels genom medverkan i ett mindre projekt som leds av Polisen i Västra Götaland, Prevention of Cargo Crimes, och dels genom ytterligare ansökningar under hösten. Vi har även slutfört vår medverkan i projektet FORESEC – Europe’s Evolving Security: Scenarios, Drivers and Trends, vars slutrapport publicerades den 16 november 2009.[3]

Samverkan MSB och Security Arena

Förutom månatliga projektledningsmöten och styrgruppsmöten som genomförts med aktivt deltagande från MSBs representanter har samverkan skett i förstudien för MSBs lägescentral, se kapitlet *Studieuppdrag*.

Specifika övriga samverkansaktiviteter har varit en inventering av europeiska referensanläggningar med inriktning mot test- och labbanläggningar inom området kritisk infrastruktur, som utförts av en arbetsgrupp för ERN-CIP (European Reference Network-Critical Infrastructure Protection). MSB har ansvarat för inventeringen av tänkbara svenska anläggningar, bl.a. genom besök till Lindholmen Science Park för presentationer av Security Arena, Chalmers och Sveriges Tekniska Forskningsinstitut (SP).

Under hösten samplanerades även en större kommunal olyckskonferens i MSBs regi på Lindholmen. Konferensen genomfördes i november med ett 100-tal medverkande och Security Arenas parter fick möjlighet att presentera exempel på genomfört arbete.

Dessutom kan nämnas att MSB och Security Arena gemensamt med Försvarsmakten planerat och genomfört ett erfarenhetsseminarium om Quickwinsexperimentet.[4] MSBs generaldirektör Helena

---

[3] Per Wikman-Svahn och Henrik Carlsen (FOI), FORESEC Deliverable D 5.4, 2009-11-26

[4] SwAF, NATO, MSB, FMV: NATO and Sweden joint live experiment on NEC, a first step towards a NEC realization, March 2009, DOP-D125-09

Lindberg besökte också Lindholmen i samband med europeiska generaldirektörers möte inom civilskydd den 10 december 2009.

Studieuppdrag

Under året initierades och genomfördes en förstudie med MSBs nationella lägescentral. Förstudien syftade både till att undersöka vilka befintliga resultat från Security Arenas arbete som är potentiellt användbara för ett eller flera pilotprojekt, men också att mer förutsättningslöst undersöka krav och behov av funktioner/förmågor som lägescentralen kan behöva på längre sikt.

I september genomfördes en tvådagars workshop med personal från lägescentralen där ett antal koncept presenterades. Resultatet av detta följdes upp under hösten och stort intresse finns för flera av de koncept som presenterades och demonstrerades i samband med den gemensamma workshopen. Följande forskningsområden och koncept följdes upp:

1. Pågående forskning inom områdena beslutsstöd och informationsdelning (Chalmers)

2. Collaboard, ett forskningsprojekt som bl.a. syftar till att öka närvarokänslan vid informationsdelning mellan geografiskt åtskilda platser (Chalmers)

3. Pågående forskning inom området informationssäkerhet (Chalmers)

4. Informationssystem, sociala nätverk samt delar av resultaten från projektet DEGEL (Saab)

5. Volatile Whiteboard, ett koncept för informationsdelning av känslig information (Ericsson)

Fortsatt uppföljning kommer att ske under 2010.

Konferenser, seminarier och demonstrationer

Security Arenas projektgrupp har under 2009 genomfört och/eller medverkat i ett flertal för verksamheten centrala konferenser, seminarier och demonstrationer, både nationellt och internationellt. Här följer några exempel:

- **Referensgruppsmöte, Lindholmen, 3 februari**
  I februari genomfördes ett större referensgruppsseminarium med ett 40-tal inbjudna referensgrupps- och expertgruppsmedlemmar. På seminariet presenterades genomfört arbete under 2008 samt planeringen för 2009. Ett antal demonstrationer genomfördes också och seminariedeltagarna gavs tillfälle till återkoppling.

- **Polisens transportsäkerhetsdag, Lindholmen, 25 mars**
  Medarbetare från Security Arena presenterade delar av arbetet med hot från organiserad brottslighet mot transportsektorn.

- **ISCRAM 2009, Handelshögskolan Göteborg, 10-13 maj**
  Under ISCRAM-konferensen presenterade medarbetare från Security Arena en fallstudie på temat: Security Arena – a Living Lab Initiative in Gothenburg.

- **Nationella telesamverkansgruppen, Lindholmen, 26 maj**
  Tillsammans med PTS (Post- och telestyrelsen) genomfördes en endagskonferens på temat hur kommersiella nätteknologier kan utvecklas och nyttjas i krissituationer. Ett 35-tal representanter från telebranschen deltog.

- **Workshop MSBs lägescentral, Lindholmen, 3-4 september**
  Inom ramen för förstudien presenterade och demonstrerade samtliga temaområden relevanta koncept och forskningsresultat för personal från MSBs lägescentral.

- **ITS World Congress, Stockholm, 21-25 september**
  Presentation av pilotprojektet Säkra och effektiva transporter genom hamn. Fyra visningar av Demoteatern med scenariot Secure Transports.

- **Euro-Atlantic Stakeholders Conference 2009, Norra Latin Stockholm, 1-2 oktober**
  Medarbetare från Security Arena presenterade delar av arbete som genomförs inom Tema 3: Surveillance and Early Warning.

- **Tolkningsseminarium, Security Arena utvärdering, Lindholmen, 13 oktober**
  I samband med utvärderingen av Security Arena genomfördes ett s.k. tolkningsseminarium med projektledningsgruppen under ledning av Faugert & Co.

- **Quickwins erfarenhetsseminarium, Lindholmen, 5 november**
  I samverkan med MSB och Försvarsmakten genomfördes ett erfarenhetsseminarium om Quickwinsexperimentet samt en diskussion om ett potentiellt fortsättningsexperiment.

- **Kommunal olyckskonferens, Lindholmen, 10-11 november**
  Ett 100-tal mötesdeltagare medverkade vid den årliga kommunala olyckskonferensen under ledning av MSB.

- **Europeisk generaldirektörsträff, Lindholmen, 10 december**
  Lindholmen Science Park arrangerade ett studiebesök för europeiska generaldirektörer inom civilskydd i samband med deras besök i Göteborg. Sammanlagt deltog cirka 140 personer vid besöket där Security Arenas verksamhet presenterades.

Under året har dessutom ett antal lunchseminarier genomförts samt ett par frukostseminarier under ledning av Combitech. Se Bilaga 1.

Övriga aktiviteter

På uppdrag av VINNOVA har ett forskningsprojekt med titeln Mobila bredbandstjänster för myndighetsanvändare genomförts under året. Chalmers har varit utförare och uppdraget kan till viss del kopplas till pågående arbete inom Tema 2: Mobilt bredband för säkerhet i samhället. Resultatet från detta uppdrag kommer att presenteras i ett separat seminarium under våren 2010.

SPECIFIKA RESULTAT INOM FORSKNING OCH UTVECKLING

Tema 1: Samhällskritiska transporter

Transporter kan liknas vid samhällets blodomlopp, detta gäller såväl till vardags som i en krissituation. Samhällskritiska transporter definieras av FOI (Totalförsvarets forskningsinstitut) som ”sådana transporter som under en given situation – om de uteblir – innebär en påtaglig risk för oacceptabla samhällskonsekvenser.”[5] Vad som då avgör en transports roll i samhället beror dels på behovet av transporten och dels på konsekvenserna av uteblivelsen av densamma.

Tema 1: Samhällskritiska transporter täcker upp flera sådana applikationsområden. Temat behandlar allt från transporter via kritisk transportinfrastruktur såsom hamnar där ett nationellt perspektiv tas i och med de godsvolymer och godstyper som hanteras, till genomförandet av enskilda transporter av farligt gods där ett flertal myndigheter har ett samhälls-, räddnings- eller sjukvårdsperspektiv – allt för att skydda och stärka samhället på bästa sätt.

Under 2009 har arbetet fokuserats på följande delprojekt:

- Delprojekt 1: Demoteatern - Säkra transporter
- Delprojekt 2: Hot från organiserad brottslighet mot transportsektorn
- Delprojekt 3: International End-to-End (E2E) Transport Security
- Delprojekt 4: Förstudie: Affärsmodeller för security-tjänster

Delprojekt 1: Demoteatern – Säkra transporter

Demoteatern är ett koncept utvecklat av Lindholmen Science Park i samarbete med NetPort, Test Site Sweden, VINNOVA, Volvo, Vägverket och Västra Götalandsregionen. Syftet för Demoteatern är att visa en bred beskrivning av ITS (Intelligent Transport System) och dess inflytande, bland annat hur säkerhet och effektivitet kan förbättras. Fyra scenarier utvecklades för att visas på Världskongressen för ITS i Stockholm 2009. Detta projekt behandlar scenariot Säkra Transporter.

[5] Lövkvist Andersen, A-L. et al. Samhällskritiska transporter. Totalförsvarets Forskningsinstitut, FOI, 2004.

Demonstrationsprojektet är baserat på det arbete som genomförts på Security Arena under åren 2005 till 2008 inom såväl farligt gods som hamnsäkerhet. Arbetet är drivet ur ett samhälls-perspektiv. Under 2009 har syftet varit att fokusera på gränssnitten mellan olika transportslag för transporter av farligt gods. Dels har en behovsanalys genomförts för att urskilja specifika problem och för att belysa krav utifrån olika regelverk.

Behovsanalys kring regelkrav vid intermodala transporter av farligt gods

Syftet med en behovsanalys är att forma en konceptuell grund för utveckling av tjänster och funktioner med specifik tillämpning inom ett område. Behovsanalysen har till största delen utgjorts av datainsamling genom intervjuer med användare och genom observationer i operativa miljöer. Ett antal intervjuer utfördes under våren och sommaren 2009 med fler än 20 intressenter från olika organisationer och företag, se Bilaga 2.

Skillnaderna i regelverk för farligt gods mellan de olika transportslagen är inte allmänt kända vilket resulterar i att de olika intressenterna inte kan agera på ett säkert och effektivt sätt kring intermodala transporter idag. Eftersom tidigare arbete har fokuserat på hamn respektive farligt gods separat har syftet med behovsanalysen varit att komplettera befintligt arbete med att identifiera behov kring säkerhet och effektivitet med fokus på gränssnittet mellan transportslagen. Tonvikten har legat på att studera krav enligt regelkrav och hur ansvarsfördelningen ser ut idag jämfört med den önskade situationen.[6] Dessutom har en existerande transportkedja analyserats för att identifiera de individuella intressenternas behov.

Ingen expertgrupp har engagerats i detta arbete utan inriktningen har legat på samarbete och utbyte inom Demoteatern. Följande partners har ingått:

- Lindholmen Science Park
- NetPort
- Test Site Sweden
- VINNOVA
- Volvo
- Vägverket
- Västra Götalandsregionen

Konceptgenerering för Demoteatern

Under tidigare år har ett antal viktiga koncept för att höja säkerheten och effektiviteten för transporter av farligt gods samt transporter genom hamnar utvecklats baserat på samhällets behov. 2009 års arbete har syftat till att vidareutveckla och kombinera dessa koncept samt att föreslå förbättringar avseende regelverken och dess tillämpning på transporter av farligt gods.

De identifierade behoven har lett till bl.a. följande behov av förändringar och satsningar:

- Tillämpa det “starkaste” regelverket och använd multimodal DGD (Dangerous Goods Declaration) avseende förpackningar, skyltar, märkning och dokumentation.
  Idag finns det inget gemensamt regelverk som reglerar hela transportkedjan.

- Ta bort övergångsperioden vid nya versioner av regelverk och presentera de nya reglerna 6 månader i förväg (som det idag görs för transporter av farligt gods med flyg). För detta

[6] Svensson, C.J. & Wang, X. Secure and Efficient Intermodal Dangerous Goods Transports. Examensarbete, Handelshögskolan, Göteborg, 2009

krävs att regelverken accepteras på nationell nivå och införs samtidigt. Då regelverken uppdateras vartannat år tillämpas ofta en övergångsperiod under 1 år då såväl det gamla som det nya regelverket är tillåtet att applicera, t.ex. så sker detta enligt IMDG (International Maritime Dangerous Goods Code). Det leder till missförstånd då olika nationer går över till nya regelverk vid olika tillfällen under detta år.

- Harmonisera eller ta bort begränsade mängder då det hanteras på olika sätt i de olika regelverken, bl.a. behövs det inga skyltar enligt ADR (Europa-gemensamt regelverk för transport av farligt gods på landsväg) och RID (Europa-gemensamt regelverk för transport av farligt gods på järnväg) medan IMDG kräver det. Svårigheten i ovanstående tre punkter ligger även i att olika regelverk har olika ansvariga organisationer som måste samarbeta, t.ex. är IMO (International Maritime Organization) på FN-nivå ansvariga för IMDG (nationellt ansvariga är Transportstyrelsen), medan ADR och RID är en överenskommelse på EU-nivå där MSB är nationellt ansvarig.

- Delat ansvar kräver holistiska kontrollplaner vilket bör koordineras av Transportstyrelsen, eftersom kontrollerna idag är ojämnt fördelade över transportkedjan såväl i frekvens som avseende dess aktörer. Idag delas ansvaret mellan flera myndigheter. Kustbevakningen (KBV) kontrollerar farligt gods till sjöss och Polisen kontrollerar vägtransporterna. Utöver detta har Transportstyrelsen det övergripande kontrollansvaret och makten för alla fyra transportslag.

- Kravet på utbildningsfrekvens bör vara två år eftersom regelverken uppdateras vartannat år och framför allt med hänsyn tagen till den ibland låga frekvens som vissa har i sina farliga godskörningar. Utbildningsnivån bör även baseras på ansvarsnivå. Utbildningsfrekvensen specificeras inte i vare sig ADR, RID eller IMDG, men i dagsläget är ADR-certifikatet giltigt i 5 år. MSB utfärdar ADR-certifikat och är därmed indirekt ansvarig (genom säkerhets-rådgivare) för att förare, transportledare m.fl. har tillräcklig utbildning om farligt gods.

- Mer resurser behövs för att kunna göra bättre kontroller av certifierade säkerhetsrådgivare. Dessa kontroller är MSBs ansvar.

- Elektronisk information istället för papper där informationssystemet varnar om felaktig information registreras vilket reducerar den stora påverkan från den mänskliga faktorn. Den senaste uppdateringen av ADR (från juli 2009) tillåter användandet av elektronisk DGD, vilket inte IMDG gör.

Uppnådda resultat för Demoteatern

En förutsättning för att skapa säkrare och effektivare transporter ligger i papperslösa transporter, vilket även är grunden i scenariot Säkra transporter. Inga nya förmågor har tagits fram i detta delprojekt, utan tidigare utvecklade tjänster har applicerats på delvis andra områden. Behoven från såväl samhälle som privata aktörer har legat till grund för utvecklingen av de scenarier som demonstrerades i Demoteatern på Världskongressen för ITS i Stockholm i september 2009. Beslutsfattare, myndigheter, potentiella partners och kunder m.fl. tog del av budskapet i scenariot Säkra transporter. Syftet är att spela upp koncept i en teatermiljö. Genom att visa komplexa system och tjänster i ett scenario med hjälp av skådespelare, teknik och rekvisita kan man öka förståelsen märkbart. Demoteatern har även filmats för dokumentation.

Huvudmålet med detta delprojekt var att nå en stor och professionell publik där en ny problembild och ett antal koncept som tillgodoser dessa behov demonstreras. En huvudingrediens var att anlita professionella skådespelare och regissör som stöttade under utvecklingen av scenariot. Under ITS Världskongressen visades Säkra transporter-scenariot fyra gånger med totalt cirka 200 åhörare med varierande bakgrund. Utvärderingen pekar på att det är ett uppskattat sätt att visualisera problem och lösningar samt att skådespelarna var en viktig del för att uppnå detta. Enligt utvärderingen för Säkra transporter tyckte 95 % att ”övergripande intryck” var ”bra” eller ”mycket bra”. Budskapet var enligt 90 % ”tydligt” eller ”mycket tydligt”. Siffrorna är från utvärderingen av Demoteatern.[7]

Delprojekt 2: Hot från organiserad brottslighet mot transportsektorn

Detta är ett nytt delprojekt 2009. Tidigare har inriktningen inom detta område varit stöldsäkerhet, vilket till största delen hittills drivits av kommersiell utveckling. Problemen med den organiserade brottsligheten medför oönskade konsekvenser i samhället och därför måste även myndigheter vara involverade i arbetet.

Godsstölder är en stor finansieringskälla för annan kriminell verksamhet i den undre världen. Smuggling, godsstölder och piratkopiering är nära sammankopplade fenomen p.g.a. att de genomförs av samma kriminella organisationer samt att de använder samma nätverk och försäljningskanaler. Enligt Polisen gäller detta också Sverige:

> ”*Transportnäringen sponsrar kriminella. Varje år stjäls gods för 1,5 miljarder kronor från lastbilar. Bara i Sverige. Vinsten från stölderna går direkt ner i fickan på den organiserade kriminaliteten. Polisen har uppmärksammat problemet, men för att stoppa dem behöver fler aktörer agera, skriver länspolismästare Ingemar Johansson och biträdande länspolismästare Klas Friberg.*”[8]

Under året har en stöldanalys av tunga fordon i Sverige utförts. Dessutom har en undersökning gjorts i syfte att kartlägga vilken typ av säkerhetsutrustning som dessa fordon var utrustade med. För att komplettera denna analys har även försäkringssituationen setts över. Resultatet är ett pilotprojekt för att demonstrera och testa s.k. remote immobilizer-teknik (fjärravstängningteknik) av lastbil och andra tjänster kopplade till ett sensornätverk runt trailer. En film har framtagits för att dokumentera pilotprojektet.

Behovsanalys av stöldsäkerhet med fokus på försäkringssidan

Enligt ovan har en analys av fordonsstölder i Sverige samt kartläggning av befintlig säkerhetsutrustning i dessa utförts. Även försäkringssituationen (varuförsäkring och ansvarsförsäkring) för de samma har undersökts. Denna översyn har utförts bl.a. genom att

---

[7] PowerPoint presentation, Evaluation Demo theatre, Volvo Technology, 2009

[8] Debattartikel, Göteborgs-Posten, 2009-10-20

intervjua representanter från två större svenska försäkringsbolag (Länsförsäkringar och IF). Det var bl.a. viktigt att undersöka om teknisk säkerhetsutrustning kan medföra lägre premier för försäkringstagarna. Dessutom har ett antal intervjuer med återförsäljare av Volvos lastbilar hållits. Syftet med dessa intervjuer var att undersöka vilken typ av säkerhetsutrustning som säljs i dagsläget samt om kunderna frågar efter dessa lösningar.

Analyserna visar bl.a. att:

- Cirka 1 % av vagnparken (tunga lastbilar) stjäls varje år. De flesta stulna lastbilar återfinns inom några dagar men cirka 10-20 % av de stulna fordonen återfinns aldrig.[9]
- Av de stulna bilarna var cirka 17 % utrustade med immobilizer (ej remote).[9]
- För 2006 var det totala premieuttaget för ansvarsförsäkring (Speditör och Transportör) från försäkringsbolagen 421 MSEK, en ökning med 99 MSEK jämfört med 2005.[10]
- För 2006 var det totala premieuttaget för varuförsäkring från försäkringsbolagen 651 MSEK, en ökning med cirka 20 MSEK jämfört med 2005.[10]
- 2007 härstammade 20,6 % av de totala ersättningskraven från försäkringstagarna från stölder eller uteblivna transporter.[10]
- Premiesättningen baseras ofta på historik och individualisering.[11] Att införa ett kraftigt premiereducerande system är svårt. Många olika parametrar påverkar/bidrar tillsammans till den totala premien vilket gör att en ny säkerhetsprodukt vanligtvis adresserar en liten del av risken, vilket medför att premiesänkningen ofta blir begränsad.

[9] P. All (2009). Truck theft investigation in Sweden, Volvo Technology, 2007-2009

[10] Försäkringsförbundet, Market statistics, The Swedish Insurance Federation, 2007

[11] Intervju med Sören Kullberg, IF, 2009-04-08

Ingen traditionell expertgrupp har deltagit i projektet. Istället har projektet anslutit sig till intressegrupperingen Transportsäkerhetsgruppen Göteborg med representanter från bl.a. branschorganisationer, åkerier, speditörer och försäkringsbolag. Bland annat driver gruppen frågan om säkra uppställningsplatser för godstransporter samt arbetar för att få upp transportköparnas intresse för säkra transporter. Arbetet utförs i nära samarbete med Polisen. Två möten har hållits under projektets gång.

Projektet har också representerats i en annan gruppering, nämligen Säkra godstransporter i centrala Göteborg. Denna grupp fokuserar på att uppnå säkra transporter vid citydistribution. Gruppen består av medlemmar som t.ex. speditörer, transportörer och branschorganisationer, se Bilaga 2. Som namnet antyder ligger inriktningen på att göra citydistributionen säkrare och minska antalet incidenter i Göteborgsområdet. Under hösten har två möten hållits.

Projektet har även gjort det möjligt att följa Restore, ett projekt som drivs i Storbritannien med syfte att utveckla remote immobilizer för högriskfordon i Storbritannien, både tekniskt och juridiskt. Det är troligt att Restore kommer att påverka framtida lösningar och hantering av remote immobilizer-teknik även utanför Storbritanniens gränser.

Konceptgenerering och utveckling av pilotprojekt

Med utgångspunkt från behovsanalysen och tidigare erfarenheter har projektet valt några tekniska artefakter att jobba vidare med. Dessa kommer att spela en viktig roll när det gäller att göra transporter säkrare i framtiden, både nationellt och internationellt. Pilotprojektet som utvecklats består av en remote immobilizer. Den möjliggör att man trådlöst, via en tunnlad Internetförbindelse, kan hindra ett fordon från att starta, sänka dess hastighet eller stänga av dess motor. Arbetet med remote immobilizer är komplext på många sätt, inte bara tekniskt, utan även när det gäller hur det kan och bör tillämpas. Att stänga ner ett 60-tons ekipage kan få dramatiska följder och det är därför mycket viktigt att samverka nationellt och internationellt för att hitta ett fungerande och hållbart regelverk.

Projektet har även arbetat vidare med trådlösa sensornätverk, vilket har resulterat bl.a. i prototyper för en trådlös panikknapp och en trådlös dörrsensor. Panikknapp och dörrsensor är i sig inga unika tillämpningar; det unika är att de är integrerade i ett trådlöst sensornätverk som förutom den uppenbara fördelen att man slipper kabeldragning även medför att det är relativt enkelt att lägga till fler sensorer eller noder i nätverket. För att övervaka och styra remote immobilizer och sensornätverket har ett webbaserat verktyg tagits fram.

För att stödja arbetet med sensornätverket har också ett examensarbete genomförts; Wireless Sensor Networks in a Vehicle Environment.[12] Inom ramen för detta arbete undersöktes möjligheten att integrera ett trådlöst sensornätverk (utvecklat av Datachassi) i ett tungt fordon med syfte att öka säkerheten för förare, fordon och gods.

Uppnådda resultat för pilotprojektet

Området Transport Security delas oftast in i tre olika delar – förarsäkerhet, fordonssäkerhet och godssäkerhet. För att skapa en säker transport är det viktigt att säkra upp alla tre delar, annars riktar brottslingarna in sig på den svagaste delen i transporten. De utvalda tjänsterna för pilotprojektet har valts för att exemplifiera lösningar och höja säkerheten för alla tre säkerhetsområden: förare (trådlös panikknapp), fordon (remote immobilizer) samt gods (elektroniskt sigill för trailer/dörrsensor). Elektroniskt sigill och trådlös panikknapp finns redan på marknaden i olika utföranden, men i detta projekt har de kopplats ihop med det trådlösa nätverket

[12] R. Basso, Wireless Sensor Networks in a Vehicle Environment, Examensarbete Chalmers, Göteborg, 2009

för att demonstrera hur man på ett flexibelt sätt kan ansluta sensorer och liknande för att få dem nätverksanslutna. Remote imobilizer har stor potential och är av stort intresse framförallt för myndigheter och är på väg att bli obligatorisk inom vissa marknader i världen p.g.a. stora problem med godsstölder.

Ett pilotprojekt har utvecklats för att testa de utvalda koncepten ovan. En film har även tagits fram tillsammans med en utvärdering av testresultatet.

Delprojekt 3: International End-to-End (E2E) Transport Security

International E2E Transport Security har varit en teoretisk fortsättning på projektet säkra och effektiva transporter genom hamn 2008. Projektet genomfördes som ett pilotprojekt för att vidareutveckla och integrera konceptlösningar, som tagits fram under 2006 och 2007. I pilotprojektet 2008 testades dessa lösningar och tjänster i transporter mellan terminal till hamn, med hjälp av ett antal aktörer. I projektet 2009 undersöktes hur de tjänster som utvecklades under 2008 skulle kunna paketeras och säljas för att få dessa säkerhetskoncept att nå marknaden. Analysen gjordes på ett utökat godsflöde från en godsterminal med lastbil och färja till en mottagande terminal i ett annat land. I delprojektet har även Saab och Chalmers deltagit.

Behovsanalys av internationella transportflöden

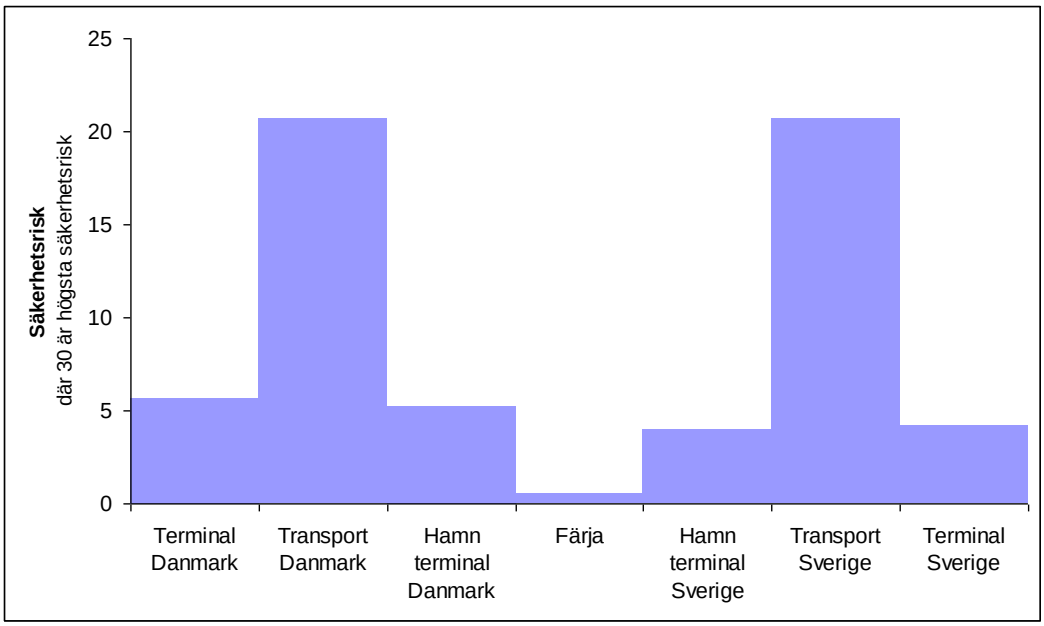
Till behovsanalysen i årets studie har materialet från 2008 kompletterats med underlag från intervjuer, studiebesök och litteraturstudier. Intervjuer har genomförts med Polisen i Västra Götaland, Tullverket och Stena Line. I december gjordes ett studiebesök till Danmark med Stena Line-färjan. Representanter deltog från Volvo Technology, Saab och Stena Line. Under besöket intervjuades kaptenen och andre styrman för att ge deltagarna en helhetssyn på säkerheten ombord och risker relaterade till lasten. I Danmark besöktes check-in till färjan för att få ett internationellt perspektiv.

Resultat av behovsanalys

Värden på säkerhetsrisk i grafen i Figur 3 är framtagna genom att lista möjliga stöldscenarier och sedan sätta en subjektiv sannolikhetssiffra på dessa scenarier (0-10) samt en siffra för värde och möjlig skada för stölden (0-3). Dessa två siffror multipliceras för att få säkerhetsrisken (max 10*3=30).

Siffrorna grundar sig på intervjuer gjorda under behovsanalysen. Hamnområden är utsatta för stölder, men varken Polisen eller Stena Line ser säkerheten på hamnområdet som det största problemet i transportkedjan. De största säkerhetsriskerna under transporten finns inte i hamnen

utan på vägen, se Figur 3. För fullständig matris över säkerhetsrisken hänvisas läsaren till Port Study Report 2009.[13]



Figur 3. Säkerhetsrisker på olika delar av terminal till terminal transport

- Terminal Sverige: Rutinerna vid inpassering till Danmarksterminalen i Göteborg skiljer sig markant från inpasseringen till Tysklandsterminalen (Majnabbe) i Göteborg där Hamnpiloten 2008[14] genomfördes. Bland annat är flödet papperslöst förutom en underskrift från föraren, där han garanterar att lasten innehåller specifikationen i bokningen. Föraren behöver inte stiga ur lastbilen vid incheckning.

- Sjötransport: Att något stjäls under sjötransporten är mycket ovanligt. Andre styrman sköter såväl pålastning som avlastning, vilket gör att han har full kontroll över det pålastade godset och vad som är farligt gods. Andre styrman tar emot dokumentation kring farligt gods vid pålastning och levererar dem vid avlastning. Endast vid transporter av farligt gods hanteras papper på Stena Line-färjan. Beledsagad trafik hanteras inte annorlunda från obeledsagad.

- Terminal Danmark: Rutiner vid check-in till terminalen i Danmark skiljer sig från dem i Sverige. I Danmark jobbar Stena Line även som speditör och har tagit över förberedelse av förtullningspapper. Tranportören skickar ett e-mail till Stena Lines kontor, där alla nödvändiga papper förbereds. Chauffören hämtar upp pappren vid check-in. Detta har lett till väntetider för att checka in, då chaufförerna måste stiga ur lastbilen för att få sina papper och pappershanteringen ofta tar lång tid. Språkliga barriärer är ett stort problem - speciellt vid tillfällen då inte förtullningspappren stämmer.

- Tullen: För att upptäcka smuggling arbetar tullen med att sätta upp riskprofiler. Huvudproblemet med lastbilstransporter idag är att tullen inte har tillräckligt med information för att sätta upp riskprofiler. Tullen har ett behov av information kring importerat gods, framför allt avsändare och mottagare.

---

[13] Hansson, F. & Westerberg, E. (2009). Port Study Report 2009. Security Arena, Lindholmen Science Park

[14] Security Arena Årsrapport 2008, Lindholmen Science Park

Tjänstepaket lämpliga för olika aktörer

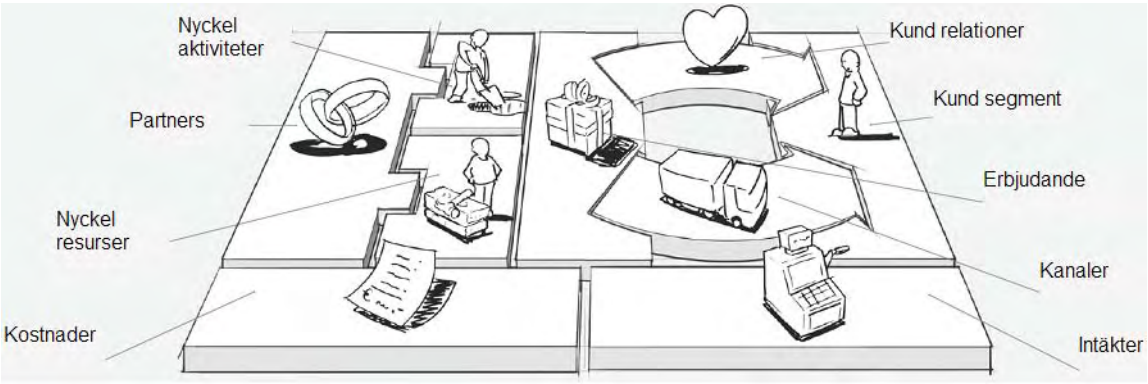
Under arbetet 2009 har inga nya tjänster tagits fram, utan en analys är gjord där de befintliga tjänsterna i 2008 års helhetslösning sätts ihop till tjänstepaket lämpliga för olika aktörer. Fyra tjänstepaket är framtagna.

- Hamn VIP: Inkluderar Internet-bokning av färja, föravisering till färjeterminal, snabb inpassering till hamnen och parkeringsanvisningar på hamnområdet.
- Säker transportstatus: Inkluderar Proof of Collection (POC), transportstatus (position och tid) och Proof of Delivery (POD).
- Tull alert: Tjänsten är ett varningssystem för tullen, baserat på anomalidetektion.
- Trailer position: En tjänst för att veta var en trailer är parkerad i en hamn eller på en terminal.

Uppnådda resultat – affärsmodeller och bedömning av säkerhetsnivåer

För att de fyra tjänstepaket som är framtagna ska kunna nå marknaden på ett effektivt sätt krävs en gångbar affärsmodell för vart och ett av dem. Tjänster som bygger på att sälja endast ökad säkerhet har varit svåra att ta betalt för, då relativt få speditörer lyckas sälja det mervärde som ökad säkerhet ger. Därför kan man kombinera tjänster som ger ökad säkerhet med tjänster som också höjer effektiviteten genom att korta transporttiden, reducera administrationen kring transportuppdraget samt höja kvalitén och leveranssäkerheten.

En ansats har tagits för att hitta bärkraftiga affärsmodeller för ökad säkerhet och effektivitet. Under affärsmodelleringsfasen användes en modell från boken Business Model Generation skriven av Alexander Osterwald och Yves Pigneur.[15] Modellen kallas The Business Model Canvas och är uppbyggd av nio block, se Figur 4. Modellen bidrar till att på ett strukturerat och visualiserande sätt ta fram affärsmodeller som är konkurrenskraftiga.



Figur 4. The Business Model Canvas

En affärsmodell för tjänstepaketet Hamn VIP har tagits fram med hjälp av The Business Model Canvas. Varje block har analyserats och detta har lett fram till en komplett affärsmodell. Det finns flera möjliga kundsegment för tjänsten och de drar på olika sätt fördel av vad tjänsten erbjuder. Stena Line är en möjlig kund, som erbjuds bl.a. reducerad pappershantering, bättre förutsättningar för planering, identifiering av förare och trailers som passerar in i hamnen. Detta gör att Stena Line har möjlighet till en obemannad check-in.

---

[15] Osterwalder, A. & Pigneur, Y, Business Model Generation, Self Published, 2009

I behovsanalysen framkom att olika hamnar har olika rutiner för inpassering och check-in. Beroende på vilken hamn som används för import/export finns olika behov av tjänsten. En annan möjlig kund är åkeriet, som får en snabb inpassering i hamnen och kan sålunda undvika väntetid i hamn.

En affärsmodell för tjänsten Säker transportstatus har också tagits fram med hjälp av The Business Model Canvas. Denna tjänst riktar sig mot åkeri och speditör. I erbjudandet ingår POC och POD och även transportstatus såsom tid och position.

Tjänstepaketen Hamn VIP och Säker transportstatus är analyserade avseende hur de påverkar transportens säkerhetsnivå. Analysen görs i en matris, där varje möjlig typ av brott på varje del av transporten analyseras med avseende på sannolikhet och värde/skada. Dessa två storheter bildar en säkerhetsfaktor. Därefter utvärderas effekten av en tjänst mot varje typ av brott. Effekten multipliceras därefter med säkerhetsfaktorn och bildar ett godhetstal för tjänsten. Summan av godhetstalen ger ett säkerhetsvärde för tjänsten applicerat på det definierade transportuppdraget. Analysen för tjänsten Hamn VIP visade att den hade ett relativt lågt säkerhetsvärde, då den inte var aktiv under den mest riskfyllda delen av transportuppdraget, dvs vägtransporten. Tjänsten Säker transportstatus däremot har mycket högre säkerhetsvärde, då den är aktiv i de riskfyllda momenten inne på terminalerna och under vägtransporten. För en fullständig matris över hur tjänsterna påverkar transportens säkerhetsnivå hänvisas läsaren till Port Pilot Study 2009.[16]

Kunderna får olika erbjudande och detta ger möjlighet till att anpassa betalningsmodell och kostnader till respektive kund. En ansats har gjorts för att se om det finns affärspotential för de fyra tjänstepaketen. Kostnader uppkommer från drift- och komponentkostnader för tjänsterna. Vid möjlighet att driva de båda tjänsterna Hamn VIP och Säker transportstatus med gemensam tjänste- och säljorganisation kommer de potentiella intäkterna från tjänsterna att överstiga kostnaderna.

Delprojekt 4: Förstudie: Affärsmodeller för security-tjänster

Målet med delprojektet var att studera affärsmodeller som skyndar på införandet av security-tjänster i transportsektorn. Detta är en utmanande uppgift på grund av den pressade transportsektorn och komplexa försörjningskedjor. Det är dock svårt att hitta en finansieringskälla, utan flera källor till finansiering behövs. Förstudien utfördes tillsammans med Ericsson och Telenor.

Slutsatsen i förstudien är att man antingen bör starta med högvärdesgodstransporter och utforma en affärsmodellspilot 2010 med representanter från nyckelaktörerna - godsägare, försäkringsbolag och TAPA (Transported Asset Protection Association) eller inrikta sig mot kollektivtrafiken och bussegmentet där möjligheterna att utnyttja reklam för att finansiera införandet av security-tjänster har mycket större potential.

Detta delprojekt har tidigare redovisats för styrgruppen för Security Arena[17] och kommer inte att redovisas utförligare i denna rapport.

Spridning av resultat

Presentationer från representanter för Tema 1: Samhällskritiska transporter kartläggs i Bilaga 1.

---

[16] Hansson, F. & Westerberg, E.. Port Study Report 2009. Security Arena, Lindholmen Science Park, 2009

[17] PowerPoint-presentation av ”Förstudie: Affärsmodeller för samhällskritiska transporter” för styrgruppen, Lindholmen Science Park, 2009-09-22

Inriktning 2010

Ambitionen för 2010 är att arbeta vidare från de erfarenheter som vi har byggt upp i Security Arena så här långt. Prioriterade fokusområden är:

- Hot från organiserad brottslighet mot transportsektorn. Fokus bör vara på helhetslösningar för att möjliggöra en uppskattning av säkerhetsnivån för hela transporten.

- Informationssäkerhet rörande transporten: Målet med vårt arbete är att på ett flexibelt sätt kunna dela information längs försörjningskedjan. Därför är det viktigt att bedöma vilka krav som bör ställas på informationssäkerheten för kommunikationssystemen i transportkedjan.

- Kollektivtrafiken med fokus på bussar: En analys bör göras för att bedöma vilka tjänster som det finns behov av i dagsläget vad gäller att skapa en trygg miljö för resenärerna. Därefter bör ett pilotprojekt formuleras, baserat på resultat från förstudien Affärsmodeller för security-tjänster.

Tema 2: Mobilt bredband för säkerhet i samhället

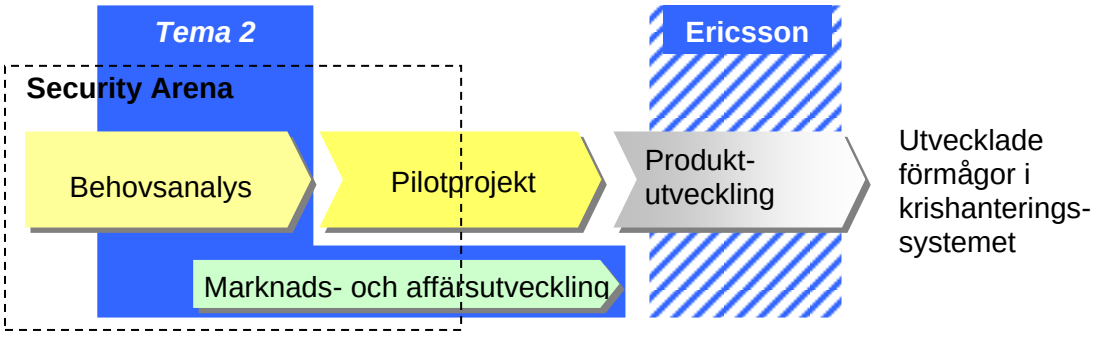
Idag lever mer än 80%[18] av världens befolkning i områden som har mobiltelefontäckning, många av dessa använder mobilt bredband med hög kapacitet. Mängden användare växer snabbt, inte minst i Afrika och Indien.

Inledning

Temat utgår från den globala mobiltelefoniutvecklingen som drivs inom ramen för 3GPP-samarbetet.[19] Arbetet fokuserar på att undersöka potentiella tillämpningar inom samhällssäkerhet och beredskap. Syfte och mål är att identifiera behov, krav och generera koncept för att utveckla förmågan hos aktörer i krishanteringssystemet.

Under 2009 har Tema 2:

- Genomfört behovsanalys, marknads/affärsutveckling och projektidégenerering
- Utvärderat förutsättningar för produktifiering av resultat från tidigare års arbeten på Security Arena



Figur 5. Tema 2 har under 2009 fokuserat på behovsanalys, affärs- och produktutveckling

Behovsanalys, marknads/affärsutveckling och projektidégenerering

Arbetet har genomförts i form av workshops och demonstrationer

- Delprojekt 1: Marknads- och affärsutvecklingsstudie tillsammans med Tema 1: Affärsmodeller för security-tjänster
- Delprojekt 2: Initiering av LiveResponse fas 3, ett samarbetsprojekt mellan Viktoriainstitutet, SAFER och Security Arena
- Delprojekt 3: Identifiering av behov inom området mobil kommunikation

Inga nya koncept har initierats.

---

[18] http://www.gsmworld.com/technology/gsm/index.htm

[19] http://en.wikipedia.org/wiki/3GPP

Delprojekt 1: Marknads- och affärsutvecklingsstudie med Tema 1

En förstudie för att utreda förutsättningar för ett pilotprojekt med säkerhetstjänster har genomförts tillsammans med Volvo och Telenor. Arbetet utmynnade i ett förslag om initiering av prov- och försöksverksamhet med applikationer för bussar. Se vidare information i Tema 1 i denna rapport.

Delprojekt 2: Initiering av projektet LiveResponse™ fas 3

Kort bakgrund

I samverkan mellan SAFER, Security Arena och Viktoriainstitutet initierades projektet LiveResponse™ hösten 2008. De prov och försök som hittills genomförts bygger på befintlig kommersiell konsumentteknologi. Resultatet har visat att det finns ett stort behov av avancerade mobila tjänster för insatsarbete. Projektet har uppskattats av medverkande aktörer som ser fram mot nästa steg i denna utveckling.

Framöver finns betydligt större krav på robusthet, integritet och kvalité, där konsumentteknologi inte är tillräckligt. Den stora ökningen av mobil bandbredd öppnar dessutom för helt nya applikationer inom området och därmed också utmaningar som behöver adresseras.

Svensk krishantering kommer i en nära framtid vara i stort behov av robust mobil bredbands-kommunikation för att på helt nya sätt organisera sig vid komplexa händelser. Redan idag ser vi exempel på innovativ användning av mobil informationsteknologi, dock i liten skala och mestadels begränsat till prov och försöksverksamhet.

Fas 3 av LiveResponse™

LiveResponse™ fas 3 startade under hösten 2009 och fortsätter under vintern för att avslutas våren 2010. Förutom Viktoriainstitutet, Security Arena och SAFER involveras bland annat Länsstyrelsen Västra Götaland, Räddningstjänsten i Stor-Göteborg, Prehospital och katastrofmedicinskt centrum VGR, MSB och Ericsson. Projektet genomförs i steg med en inledande behovsanalys följt av pilotprojektutveckling samt en avslutande prov och försöksperiod.

För pilotprojektet utvecklades en applikation för innovativ användning av live-video i mobila och stationära ledningsfunktioner. Denna applikation ska senare utvärderas genom skarp provdrift mellan mobilstab, mobil insatsledning och ledningscentral. Syftet är att prova hur användning av högkvalitetsvideo bidrar till en förbättrad möjlighet att få en gemensam lägesuppfattning vid en räddningsinsats.

Projektet kommer att dokumenteras med filmsekvenser och rapport som beskriver utfallet av genomfört pilotprojekt.

Delprojekt 3: Identifierade behov inom området mobil kommunikation

Delprojektet har genomförts workshops och demonstrationer i samverkan med:

- Mobile World Congress 2009
- PTS och Nationella Telesamverkansgruppen
- MSB och EU-gruppen för implementering av VMA med Cell Broadcast
- Förberedelser inför Mobile World Congress februari 2010

Arbetet har identifierat:

- Behov av förstärkt datakapacitet i RAKEL
- Behov av lösning för varning och information till allmänheten via mobiltelefoner

Behov av förstärkt datakapacitet i RAKEL

Dagens myndighetsägda mobila nät erbjuder i huvudsak tjänster för talkommunikation och datakapacitet på 4 – 7,2 kbps. Erfarenheterna från tidigare arbete på Security Arena visar att data-relaterade tjänster i många fall behöver 10-100 gånger högre datakapacitet. Exempel på sådana tjänster är video-applikationer och gemensam lägesbild mellan aktörer på fältet och ledningscentral.

Behovsanalysen har utmynnat i ett identifierat behov av att förstärka datakapaciteten i RAKEL.

Behov av lösning för varning och information till allmänheten via mobiltelefoner

Idag är mobiltelefonen var mans egendom, därmed skulle mobiler kunna användas för att sprida information till befolkningen och på så vis bidra till ökad säkerhet och beredskap i samband med olyckor, katastrofer och kriser. Erfarenheter från katastrofer som tsunamin i Indiska oceanen, orkanen Katrina i USA och översvämningarna i centrala Europa har också påvisat att de mobila terminalerna underlättar kommunikation vid räddningsinsatser. En fördel med mobiltelefonsystem i förhållande till fast telefoni är att mobiltelefonsystemen oftast är snabbare och lättare att återupprätta efter ett bortfall.

Behovsanalysen har utmynnat i ett identifierat behov av metoder för varning och information till allmänheten via mobiltelefoner.

Utvärdering av förutsättningar för produktutveckling

Ericsson har i enlighet med Security Arenas process under året arbetat med att utvärdera förutsättningar för produktutveckling av resultat från tidigare års arbeten. Identifierade koncept befinner sig nu i olika stadier:

- Grupp-Radio över Cellulära nät (GRS) (demonstrerades 2008) planeras bli tillgänglig på marknaden från och med våren 2010.
- SIMSEC (demonstrerades 2008 och 2009) är numera tillgänglig på marknaden.

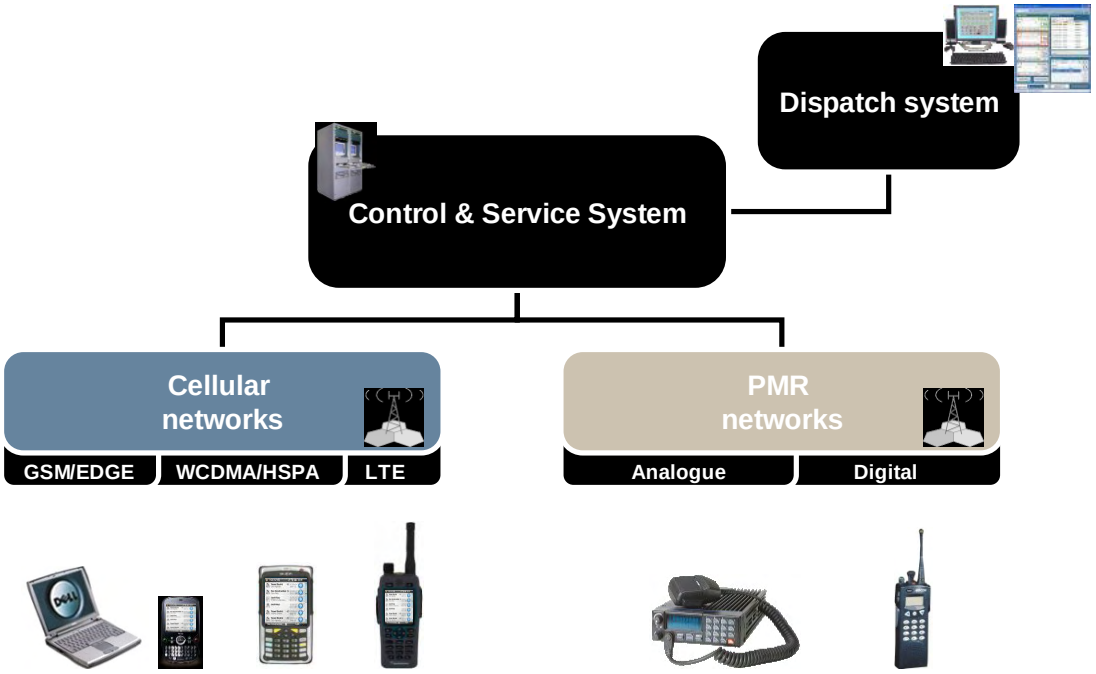
Grupp-Radio över Cellulära nät (GRS)

Traditionellt kommunicerar myndighetspersonal över walkie-talkie-liknande radionät. Denna tradition med växelvis enstaka talare som avlyssnas av ett stort antal mottagare har över åren också genomsyrat myndigheternas arbetsmetodik. Det är viktigt att inte allt för drastiskt tvinga fram

en ändring i användarnas arbetsprocess genom införandet av nya kommunikationsverktyg. De etablerade funktionerna måste fortsätta att vara tillgängliga, men kompletteras av moderna och effektivitetshöjande funktioner.

Från tidigare faser på Security Arena har behov identifierats av förstärkt täckning (yta) och kapacitet. Dessa behov har resulterat i GRS.

GRS demonstrerades 2008 och planeras kunna levereras som färdig produkt under våren 2010. Konceptet är framdrivet ur en idé att kunna erbjuda sömlös interoperabilitet mellan TETRA (TErrestrial Trunked RAdio) och professionell gruppkommunikation via mobilnäten.



Figur 6. Generell arkitektur för GRS

GRS 10A[20] erbjuder alla de tjänster som normalt är tillgängliga i dagens Private Mobile Radio (PMR) system, t.ex. push-to-talk (PTT) grupp-kommunikation, nödsamtal, gruppskanning, Late Call Entry, prioritet/override, caller ID, Presence (status) & location, text-meddelanden, Dispatch Command & Control. Men framför allt erbjuder GRS sömlös kommunikation mellan befintliga PMR-nätverk (RAKEL, S70/S80, etc.) och publika mobilnät, dvs kommunicera utanför PMR-nätets gränser via mobilnätens nationella och internationella roaming-möjligheter.

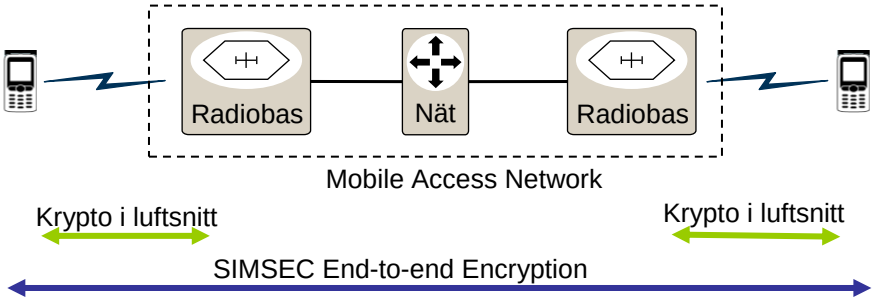
SIMSEC

Från tidigare faser på Security Arena har behov identifierats av säker och diskret talkommunikation. Dessa behov har genererat SIMSEC.

SIMSEC är ett koncept med syfte att täcka det säkerhetshål som kan uppstå då mobilnätens interna kommunikation är helt beroende av operatörernas skalskydd. SIMSEC ger säker, upp till NATO-konfidentiell kommunikation, genom end-to-end kryptering, mellan två personer över publika och internationella mobilnät.

---

[20] Vid utveckling av produkter inom Ericsson betyder 10A första (A) revision tillgänglig på marknad år 2010, nästa release skulle heta 10B om den släpps under 2010 eller 11A om den blir tillgänglig år 2011.



Figur 7. Kryptering med och utan SIMSEC

Uppnådda resultat och utveckling av tidigare koncept

Ett prov- och försöksnät för mobil kommunikation, licensierat till Lindholmen Science Park av PTS, har sedan 2006 levererat täckning kring Lindholmen och Mölndal. Det mobila nätet har använts för test, prov och försök vid utvecklingen av koncepten GRS, SIMSEC, VMA (Viktigt Meddelande till Allmänheten) över Cell Broadcast etc.

GRS- och SIMSEC-koncepten visades i februari på MWC09 (Mobile World Congress 2009) i Barcelona. MWC är världens största mässa och konferensarrangemang för mobiltelesystem-leverantörer och operatörer[21] med över 47 000 besökare 2009. I februari kommer Ericsson att visa både GRS och SIMSEC på MWC, som även 2010 äger rum i Barcelona.

GRS-konceptet har utvärderats av den australiensiska telekomoperatören Telstra i det nationella nätet.

Konceptet VMA över Cell Broadcast har demonstrerats för EU-projektet Cell Broadcast for Public Warning inom ramen för regeringsuppdraget till MSB (dåvarande RV & KBM, dnr 2005/2888/CIV). EU-projektet består av deltagare från sex länder (Tyskland, Ungern, Holland, Polen, Storbritannien och Sverige). Kärnan i demonstrationen var att illustrera egenskaperna i existerande Cell Broadcast-mekanismen, t.ex. förmåga att distribuera textmeddelande till samtliga mobiler inom ett angivet område under två sekunder.

På begäran av PTS har en resultatredovisning och demonstration genomförts för den Nationella Telesamverkansgruppen. Utöver presentation av identifierade behov, krav och genererade koncept genomfördes konceptdemonstrationer av GRS, SIMSEC, QuicLINK och VMA.

Inriktning 2010

Inför kommande år föreslår Tema 2 studier inom följande områden:

- VMA – identifiera behov och generera koncept
- Förstärkt RAKEL – initiera praktiskt GRS-prov (pilotprojekt) med kommersiella mobilterminaler och RAKELs TETRA-nät
- Initiera ett pilotprojekt baserat på resultaten från förstudien Affärsmodeller för security-tjänster (se Tema 1, delprojekt 4)

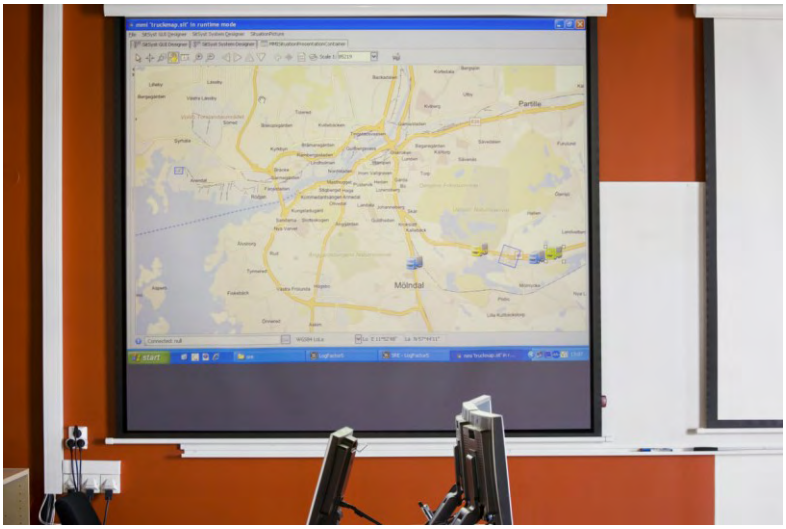
[21] http://en.wikipedia.org/wiki/Mobile_World_Congress och http://www.mobileworldcongress.com

Tema 3: Surveillance and Early Warning

En effektiv krishantering, dvs en krishantering som förhindrar vidare eskalering hanterar det uppkomna läget samt bidrar till en snabb återgång till ett ”normalläge”, kräver att alla inblandade har tillförlitliga beslutsunderlag och effektiva beslutsstöd. Nyckeln till detta ligger i att skapa en beredskap i den dagliga verksamheten. Om operatörer och samhälle skall vara tillräckligt starkt motiverade till att satsa större resurser på krishantering och tidiga varningssignaler måste dessa system och processer även stödja den vardagliga verksamhetens effektivitetsmål.

Detta tema behandlar övervakning av samhällskritiska infrastrukturer, i syfte att så tidigt som möjligt ge varning vid risk för eskalerande kriser i samhället. Tema 3 bidrar därmed aktivt till att höja samhällets krisberedskap genom att studera tekniker och metoder för att stödja samverkan på alla nivåer i krishanteringssystemet.

Arbetet under 2009 grundar sig på det framarbetade konceptet att med hjälp av informationsinsamling skapa en Gemensam InformationsArea (GIA). GIA utgör en grund för tjänster som informationsfusion, informationsanalys och informationsspridning vilket underlättar krishanteringen för olika aktörer i krishanteringssystemet.



Information Flow Management

Flödet av information mellan olika aktörer är en förutsättning för att man snabbt och effektivt ska kunna återgå till ett kontrollerat normalläge om en kris uppstår. Projektet Information Flow Management (IFM) inriktar sig på olika aspekter när det gäller informationsflöde och bygger på tidigare arbeten (2007 och 2008) inom Security Arena och då främst inom den verksamhet som genomförts i projektet Secure and Efficient Port Operations (SEPO).

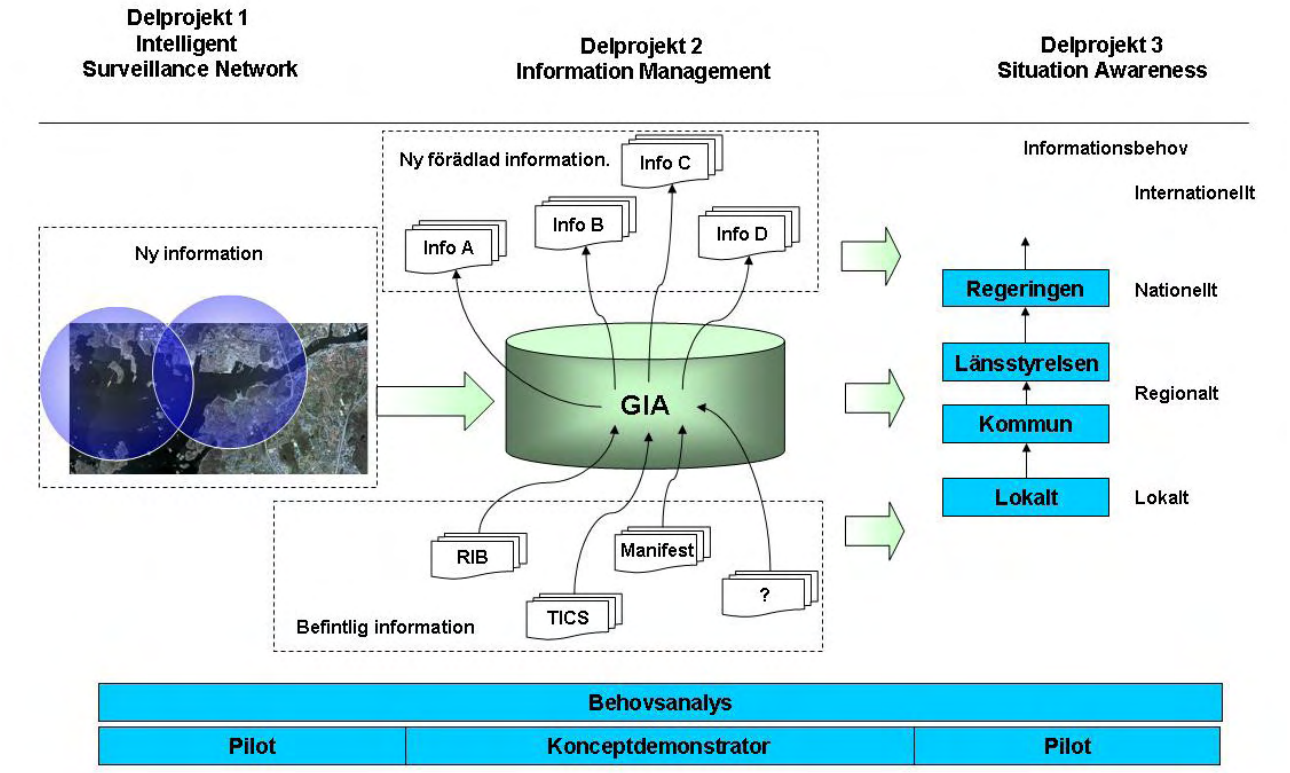
IFM är ett tvärtematiskt projekt, med huvudfokus i Tema 3. Detta innebär att vissa delar passar även in i andra teman på Security Arena. Det centrala i IFM är GIA där information samlas in, förädlas, kombineras och distribueras. IFM är indelat i tre autonoma men sammanhängande delprojekt:

- Delprojekt 1: Intelligent Sensor Network (ISN) - tillhandahåller information avseende områdesövervakning och bidrar, konceptuellt, till GIA genom rapporter på larm och andra händelser från det övervakande området. Denna information är också användbar för andra aktörer än just de som är i direkt anslutning till det övervakade området (situationsberoende).

- Delprojekt 2: Information Management - behandlar hur information kan insamlas, vilka som producerar/konsumerar information samt identifierar nya intressenter, aktörer, hotbilder/risker och teknikområden med kopplingar till fraktmanifest. Detta delprojekt har stark koppling till Tema 1, Samhällskritiska transporter.

- Delprojekt 3: Situation Awareness - undersöker hur information kan delas och hur samverkan kring informationsdelning kan fungera och realiseras. Här finns även fokus på resurserna som delar information och inte bara informationen i sig.

Delprojekt 1 och Delprojekt 3 har under året utförts som pilotprojekt. Delprojekt 2 har genomförts som en konceptdemonstrator. Samtliga delprojekt har gjort en behovsanalys för att skapa rätt förutsättningar för genomförandet.



Figur 8. Information Flow Management (IFM)

IFM är ett nationellt drivet projekt. Projektets medlemmar befinner sig på olika orter runt om i Sverige (Skövde, Göteborg, Linköping, Helsingborg, Järfälla, Stockholm, Arboga) och bidrar med kompetens och domänkunskap inom olika områden. Detta medför också att aktörer från olika delar av Sverige finns med i projektets expertgrupper.

Delprojekt 1: Intelligent Surveillance Network

Intelligent Surveillance Network (ISN), tidigare även kallat Area Protection Network (APN), är ett på Saab framtaget systemkoncept för områdesövervakning. Konceptet integrerar, behandlar och utvärderar information från olika sensorer, med avsikt att ge dess användare en ökad situationsförståelse i samband med olika typer av övervakningsuppdrag.

ISN utgör Delprojekt 1 i IFM och består av två delar. Den första delen är en behovsanalys och en scenariobeskrivning. Den genomförs tillsammans med en expertgrupp, vars uppgift är att ge synpunkter på föreslaget ISN-koncept samt ge förslag på scenarier och användarfall som är relevanta för deras verksamheter. Den andra delen består av ett pilotprojekt, som innebär en realisering och demonstration av ISN utförd på testplats Kallebäck, Göteborg.

Behovsanalys mot konceptet för intelligent områdesövervakning

Saab har en lång och gedigen erfarenhet av utveckling av militära produkter och system. En god kännedom av vad kunden vill ha och vilka krav denna ställer på utvecklade produkter är oftast given, då utveckling sker i en dialog med kunden. Så är inte fallet för nya produkter som tas fram för den civila marknaden. Här gäller snarare att produkten utvecklas först och säljs sedan. För att säkerställa att rätt produkter utvecklas, med förmågor som kunden efterfrågar och med prestanda som är anpassad till en annan prisbild jämfört med vad som gäller för den militära domänen, genomfördes en behovsanalys inriktad mot konceptet för intelligent områdesövervakning under hösten 2009.

Det primära syftet med genomförd behovsanalys är att diskutera Saabs koncept för områdesövervakning och låta en expertgrupp ge synpunkter på hur ISN kan användas inom olika områden och vilka förmågor som är önskvärda. Den framkomna behovsbilden ligger sedan till grund för utformningen av förmågor och funktioner i pilotprojektet.

En expertgrupp bestående av olika aktörer, intressenter och användargrupper har identifierats och satts samman. Behovsbilden för ISN har etablerats genom intervjuer med expertgruppen, som kom att bestå av representanter från Göteborgs hamn (Thomas Fransson), Preem (Kristian Fred), Securitas (Johan Ohlsson), Peab (Peter Martin), Tullverket (Jan-Ivar Andersson) och LFV Landvetter (Dan Larsson). De har i huvudsak en lokal förankring i Göteborgsområdet. Några av dem har dessutom varit med i tidigare projekt som genomförts på Security Arena. Ytterligare relevant information för ISN har samlats in via kontakter med Got Event (Åke Söderberg) och Länsstyrelsen i Västra Götaland (Bengt-Arne Bom).

Under genomförda diskussioner med expertgruppen framkom bland annat följande:

- *Varför övervakas området?*
  Den vanligaste anledningen till att ett område övervakas är att förhindra och försvåra möjligheten att utföra olika typer av brott, vanligtvis stöld och svinn, inom området. Incitamentet för att ha en hög säkerhet är emellertid relativt lågt då varor och gods oftast är försäkrat och hög säkerhet medför hög kostnad. För vissa områden, som t.ex. Göteborgs hamn, ställer regelverk och myndigheter krav på en viss säkerhetsnivå. Ingen av de intervjuade upplevde någon hotbild från terrorister.

- *Vad övervakas?*
  Behörighet hos personal gällande in- och utpassering till område kontrolleras ofta. Dock är övervakning inom området vanligtvis begränsad, men önskvärd. Det samma gäller införsel av fordon och gods.

- *Vilken typ av insats efterfrågas?*
  Övervakningen sker väldigt ofta i avskräckande syfte, där ingen egentlig insats utförs. Det fungerar då främst preventivt och tjuvar gör sig inte besväret. Väktare vill göra insats endast mot verifierade larm. Ett robust och användarvänligt system med få falsklarm är därför önskvärt. Tiden är ofta en viktig parameter vid larmhantering. Ett larm som kommer tidigt (Early Warning) skapar goda möjligheter att kunna vidta rätt åtgärder.

- *Övervakningsprinciper*
  Ett system som presenterar all relevant information är önskvärt. Ofta finns separata system som arbetar parallellt. Vanligaste sensorer är kameror och RFID-kort. Radarer med allvädersförmåga används inte i dagsläget. Övervakningen utförs till största delen manuellt. Beslutsstödsfunktioner såsom anomalidetektering finns inte.

- *Problem med områdesövervakning*
  Största problemet är att övervakning är dyrt. Ibland är gällande lagstiftning också ett

problem. Det gäller främst hantering av kameraövervakning på allmän plats samt hantering av inspelat bildmaterial och personuppgifter.

- *Framtida behov*
  Framtida behov inkluderar sensorer med allvädersförmåga, ett system istället för flera parallella system, robusta system med få falsklarm, möjlighet att adaptiv styra tillgängliga resurser, beslutsstödsfunktioner av typen anomalidetektering, mobila säkerhetssystem för särskilda händelser, spårning av personer, fordon och gods inom området.

Konceptgenerering

ISN är ett generiskt övervakningssystem för all typ av områdesövervakning och skalskydd, applicerbart på land såväl som till sjöss. Systemet är utvecklat runt en integrationsplattform till vilken en mängd olika sensorsystem och mjukvaruapplikationer kan knytas. Data från olika källor sammanförs till en gemensam lägesbild. Användaren kan därför fokusera på en samlad översiktsbild som innehåller all relevant information. Intelligensen i systemet består då i huvudsak av förmågor som inte bara detekterar och följer på mål inom området, utan även på förmågor som automatiskt utvärderar lägesbilden med avsikt att upptäcka eventuella hot och anpassa tillgängliga sensorresurser därefter.

Radarer och kameror används primärt för detektion och följning av olika objekt (människa, gods eller fordon). Fusionerad data från olika objekt presenteras för användaren på en kartbild i form av målsymboler. Dessa visar var på kartan som en händelse utspelar sig och hur målen förhåller sig till varandra och sin omgivning. När ett objekt bryter mot tillträde på plats uppmärksammas operatören om händelsen och en kamerabild kan visa vad som sker på den aktuella platsen. ISN inkluderar även en funktion för detektering av avvikande beteende, så kallade anomalier, i lägesbilden. Anomalier kan detekteras antingen med regelbaserade (exempelvis in/utpassage genom fördefinierade zoner) eller självlärande metoder.

Uppnådda resultat och pilotprojekt

Under året har Saab studerat ett nytt koncept för områdesövervakning som går under namnet ISN. Ett sådant system kan bidra med en mängd förmågor som tänkta användare av systemet efterfrågar. Genomförd behovsanalys har identifierat ett antal förmågor som är unika för ISN. Systemet hanterar enskilda heterogena sensorer och ger användaren möjlighet att hantera larm för avvikande situationer eller beteenden som kan utvecklas till reella hot. En gemensam lägesbild med all relevant information presenteras. En operatör slipper därför leta information från olika parallella system med sina respektive presentationsgränsytor. Ingående radarsensorer ger systemet allvädersförmåga, vilket är unikt. En radarsensor med sina goda egenskaper såsom stor täckningsförmåga, hög avståndsupplösning samt förmåga att detektera rörliga mål, kompletterar

dessutom kameran som inmätande sensor, även under goda ljusförhållanden. Ingen av de intervjuade i expertgruppen hade någon erfarenhet av radar som övervakande sensor.
ISN realiserades i form av ett pilotprojekt fysiskt på testplats Kallebäck. Testplats Kallebäck är ett område på cirka 20 000 m^2 som innehåller tillfartsvägar, parkeringsområden och stängslade områden dit allmänheten inte har tillträde. Ingående sensorer är tre stycken CCTV kameror från AXIS, en PTZ-kamera och tre stycken SIRS radarer (Saab Intelligent Radar Sensor). ISN kan fjärrkopplas via Saabs demonät (SPINE) till valfri punkt i nätet. Lindholmen Science Park utgör en nod i Saabs demonät för att ISN ska kunna demonstreras live.

ISN konceptets förmågor som demonstrerades i pilotprojektet inkluderade:

- ISN upptäcker, positionerar och realtidsföljer kontinuerligt alla objekt i det övervakade området, oberoende av väder- och ljusförhållanden (24 juli).
- ISN genomför sömlös och entydig följning över hela området med bibehållen identitet på följda objekt.
- All information korreleras och sammanställs till en gemensam lägesbild som visas på en karta över området.
- Lägesbilden hotutvärderas automatiskt och kontinuerligt.
- Användaren kan fokusera på intressanta områden och händelser genom adaptiv sensorstyrning.
- ISN kan skilja ut egen personal och andra resurser i lägesbilden.

Ovanstående förmågor demonstrerades i pilotprojektet i form av ett antal tillämpningsfall som bedömdes vara intressanta från användarhåll.

Delprojekt 2: Information Management

Behovet att dela information på ett enklare och effektivare sätt ökar i takt med att den tekniska utvecklingen möjliggör spridning av information. Samtidigt har aktörer valt att utveckla olika interna lösningar som stödjer de egna processerna. Utvecklingen av regelverk och krav, såväl nationella som internationella (EU), medför att det uppstår nya informationsbehov kopplade till de logistiska flödena från myndigheter. Samtidigt exponeras transporter och gods för kriminell verksamhet över hela världen där avsaknaden av en samlad informationsbild försvårar brottsbekämpningen.

Delprojektet vill med denna studie identifiera behov och möjligheter bland myndigheter och aktörer som utsätts för risker och krav i de logistiska flödena. Syftet är att ta fram fakta som kan ligga till

grund för nya informationskoncept. Studiens fokus är stöldproblematiken och möjligheter kring informationsutbyte för att stärka olika delar av transportsektorn, både för den privata transportbranschen och berörda myndigheter.

Behovsanalys av informationsbehov för transportsäkerhet

Delprojektet genomförde en behovsanalys som utökar tidigare genomförda arbeten (2007 och 2008) inom Security Arena, främst inom den verksamhet som genomförts i projektet Secure and Efficient Port Operations.

Syftet med behovsanalysen var att identifiera nya intressenter, aktörer, hotbilder/risker och teknikområden med kopplingar till fraktmanifest. Behovsanalysen skulle också identifiera nya informationskällor och ta hänsyn till hur information hanteras i dagens logistikflöden. Arbetet genomfördes under antagandet att förädlad information ska kunna nyttjas inom flera områden med kopplingar till brottsbekämpning och övervakning av logistikflöden. Ett typiskt sådant flöde är farligt gods, ett annat stöldbegärligt gods.

Transportstölder är ett problem i dagens samhälle, även om det i relation till andra områden kan tyckas mindre viktigt. Det har konstaterats att kostnaderna för stölderna omfattar miljardbelopp och Polisen har en ambition att minska dessa. Det finns många kända åtgärder för att komma tillrätta med stöldproblematiken, men inom branschen anses de oftast vara olönsamma att införa.

Ett antal intressenter och aktörer som är intresserade av att ta del av information, som skulle kunna tillhandahållas via en Gemensam InformationsArea (GIA) har identifierats. Intervjuer har genomförts med representanter för Schenker, Larmtjänst och polisen i Västra Götaland. Ytterligare information har samlats in via kontakter med bland annat Vägverket, MSB och Enköpings Åkeri.

En sammanfattning av informationsbehovet inkluderar följande:

- Speditörer och åkerier är intresserade av trender rörande transportstölder. GIA skulle här kunna ge en samlad bild som enskilda aktörer inte själva har möjlighet att se utifrån endast sitt perspektiv.

- Myndigheter har intresse av att få tillgång till mer detaljerad information om transporter och i många fall kunna få ta del av denna information medan den fortfarande är aktuell. En GIA som har tillgång till information från flera aktörer kan vara ett verktyg som producerar denna informationsbild. Baserat på informationsbilden kan både kontroller utföras och statistik beräknas.

- Försäkringsbolag och Polisen saknar i många fall information om vad som stjäls, vilket minskar deras effektivitet att vidta rätt åtgärder. Förbättrad information om saknat gods är därför vitalt för deras arbete.

- Standardiserade gränssnitt mellan olika system och ett mer enhetligt regelverk underlättar utbyte av information från fraktmanifest och fraktsedlar. Eftersom det finns en mängd system och branschen inte alltid ser egennyttan med anpassningar, skulle en GIA fungera som ett informationsnav. Många format skulle hanteras, vilket minimerar behovet av aktörernas systemanpassningar.

Ytterligare information som kan tas in i GIA-konceptet inkluderar realtidsinformation om transporter längs med vägarna och vid gränspassager. Vid behov ger det kunskap om vilka fordon som passerar och vilken typ av gods de för med sig. Denna information skulle kunna samlas in, dels av befintliga kamerasystem och dels av nya typer av avläsningspunkter. En begränsning är att befintliga kamerasystem i dagsläget inte får användas för ändamål som de inte är avsedda för.

Konceptgenerering via seminarier och workshops

För att utveckla och bekräfta resultatet från behovsanalysen har delprojektet genomfört en heldag med seminarier och workshop i Göteborg. Syfte med denna dag var att konkretisera möjligheterna med GIA. Följande myndigheter och aktörer, som deltagit i projektet mellan 2007 och 2009, var inbjudna: Schenker, DHL, Enköpings åkeri, Larmtjänst, Polisen i Västra Götaland, MSB, Tullverket, Lunds Universitet (NGIL) och Volvo Technology.

Vi ville med denna dag föra samman olika myndigheter och aktörer för att tillsammans utveckla idéer och möjligheter, och utifrån några scenarier identifiera gemensamma beröringspunkter där informationsdelning kan lösa nutida och framtida behov. Konkret syftade dagen till att identifiera ett reellt behov av en GIA och att undersöka de olika aktörernas villighet att tillgängliggöra information för att skapa effektivare möjligheter för informationsutbyte och informationsförädling.

Uppnådda resultat

Med behovsanalysen har delprojektet identifierat ett antal intressenter och aktörer som är intresserade av att ta del av information som skulle kunna tillhandahållas via GIA. Bearbetad information kan användas för att fylla det behov som finns angående aktuella trender rörande exempelvis transportstölder, förbättring av möjligheterna att kontrollera transporter och underlätta framtagande av statistik. GIA kan hjälpa försäkringsbolag och Polisen att snabbt få information om vad som stjäls, vilket medför att de mer effektivt kan vidta rätt åtgärder.

GIA-konceptet introducerar en förmåga att utbyta information från exempelvis fraktmanifest och fraktsedlar och fungerar som ett informationsnav som kan hantera information från många format, vilket minimerar behovet av aktörernas systemanpassningar. Detta är viktigt eftersom det finns en mängd system och branschen inte alltid ser egennyttan med anpassningar.

Ytterligare information som kan tas in i GIA-konceptet inkluderar realtidsinformation om transporter längs med vägarna och vid gränspassager för att veta vilka fordon som passerar och vilken typ av gods de för med sig. Denna information skulle kunna samlas in dels av befintliga kamerasystem och dels av nya typer av avläsningspunkter.

GIA kommer att kräva regler för vilka som kan utnyttja vilken typ av information. Genom att sätta samman GIAs information i nya informationsmängder kan de olika aktörernas behov och intressen tillfredställas. Detta kan ske genom bl.a. klassificering av informationen, identifiering av aktörer och intressenter i olika nivåer och slutligen i form av anomalidetektion.

Sammanfattningsvis kan det konstateras att mycket relevant information finns i de administrativa systemen som genererar fraktmanifest, frakt- och ordersedlar samt i system hos berörda myndigheter och organisationer. Genom att knyta ihop denna informationsmängd och göra den tillgänglig förenklas möjligheten att komma åt viktig data för brottsbekämpning, hitta aktuella trender och ge visibilitet åt aktörer för ökad kontroll av godset och godsflödet.

Genom delprojektets heldag med seminarier och workshop i Göteborg har vi fått bekräftelse att det finns behov av nya lösningar för informationsåtkomst och -delning. Dock ställs det krav att detta kan ske på ett kontrollerat sätt och att lösningen är internationellt applicerbar.

Delprojekt 3: Situation Awareness

Att undersöka metoder och skapa verktyg för att organisationer ska kunna skaffa sig en gemensam lägesuppfattning är ett huvudmål för verksamheten inom delprojektet. Metoderna och verktygen måste vara tillräckligt generella så att olika myndigheter och organisationers behov ska kunna tillgodoses. Det gäller på samma sätt att rapporteringsmöjligheter, lägesbilder och verktyg även ska kunna användas av projekten som drivs på Lindholmen.

Saab använder ofta begreppet Situation Awareness men ett alternativt och mer omfattande begrepp är Sensemaking – Situation awareness motsvarar en lägesbild, Sensemaking handlar om att förstå lägesbilden och se dess helhet. Saab har fortsatt att återanvända den kunskap och de slutsatser som gjordes i DEGEL-projektet[22] för KBM/MSB. DEGEL står för Demonstrator Gemensam Lägesuppfattning och detta projekt undersökte metoder och arbetssätt för att skaffa, bibehålla och sprida en gemensam lägesbild ur ett lokalt, regionalt och nationellt perspektiv (Slutrapporten för DEGEL är i skrivande stund inte fastställd av MSB). Följande har Wikipedia att säga om begreppen Situation Awareness och Sensemaking:

> *"In organizations, sensemaking is a collaborative process of creating shared awareness and understanding out of different individuals' perspectives and varied interests. The process of moving from situational awareness in individuals to shared awareness and understanding to collaborative decision-making can be considered a socio-cognitive activity in that the individual's cognitive activities are directly impacted by the social nature of the exchange and vice versa."*[23]

Begreppen antyder att med en delad lägesbild och med möjligheter att kommunicera kring lägesbilden kan man förstå lägesbilden och skaffa sig en gemensam lägesuppfattning och sedan ta beslut, prioritera åtgärder och sätta upp gemensamma mål.

Med koppling till DEGEL och Saabs koncept inom nationell krishantering SAE (Situation Awareness Engine) har en server med tjänster för rapportering, lägesbild och Secure Social Web driftsatts. Tillsammans med MSB och aktörer kommer Saab att ytterligare utvärdera verktyg och arbetssätt för att hantera komplexa situationer i vardag och i kris. Denna provdrift går nu under namnet Sensemaking Engine Demonstrator (SMED) och är tänkt att vara en skarp variant av DEGEL och samtidigt uppfylla som har efterfrågats under vår behovsanalys 2009.

Behovsanalys – behov av samverkan

I behovsanalysen är kopplingen till DEGEL central. Projektgruppen har i Lindholmens regi kunnat fortsätta att diskutera med aktörer om vilka behov som finns. Projektgruppen har fått möjlighet att föra samtal med olika organisationer som även är intresserade av det dagliga användandet.
Hur man får myndigheter och organisationer att samverka i vardagen ser projektgruppen som en av nyckelfrågorna som behöver lösas. Inom kommuner och länsstyrelser finns samverkansbehov – den ena handen vet inte vad den andra gör. Projektgruppen har konstaterat att kriser uppstår när samverkan misslyckas.

Organisationer behöver dagligen utbyta information och öka samverkan eftersom nya och mer komplexa beroenden i samhället skapas. När samverkan, samordning och samarbete fungerar inom och mellan organisationer och myndigheter under vardagsförhållanden kommer de förnuftsmässigt att fungera bättre under kris. Om verktyg för samverkan i vardagen tas fram ger detta även en möjlighet att bredda användningsområdena. Därmed ökas chanserna för att industrin ska kunna ta fram ett nationellt och internationellt krishanteringsverktyg.

---

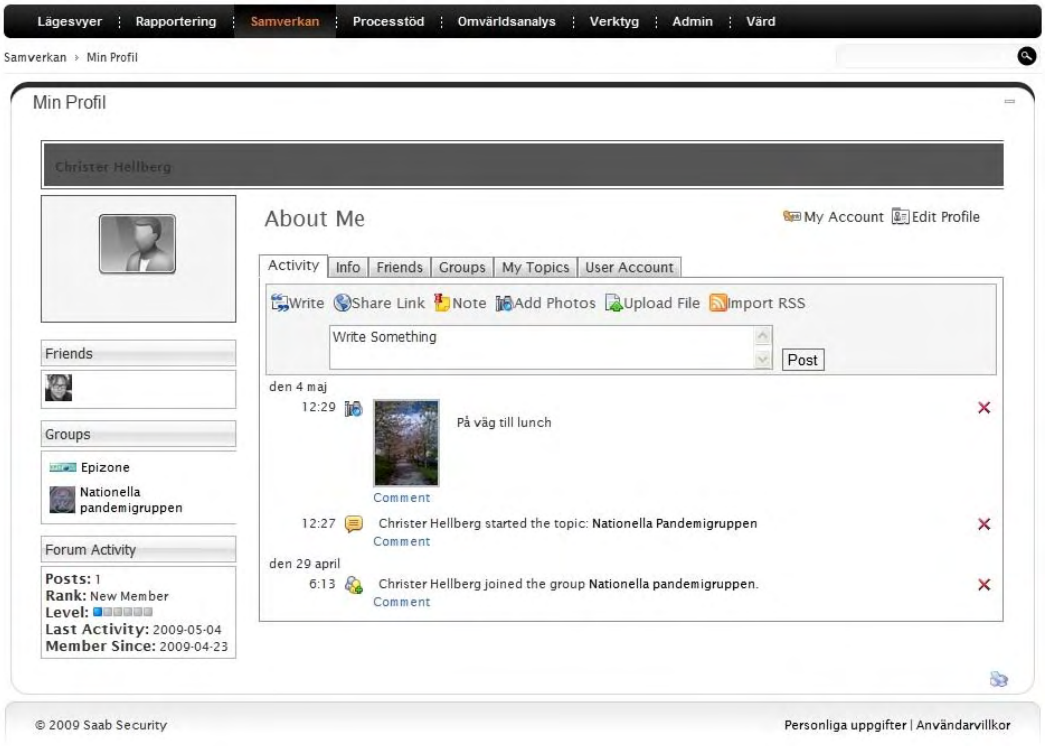
[22] DEGEL pågick under 2007-2009 och ledde till två demonstrationer av förmågor som visar en gemensam lägesbild under kris på olika nivåer i samhället – från kommunalt perspektiv till nationellt. Första demonstrationen inriktade sig på ett SAMÖ-scenario och den andra på ett pandemiscenario. DEGEL visade på arbetssätt och gav förslag på verktyg och metoder som används i nuvarande system inom domänspecifika lösningar för att visa lägesbilder inom t.ex. el, tele, trafik och sjö.

[23] http://en.wikipedia.org/wiki/Sensemaking

Teknik för ökad samverkan

Under behovsanalyser inom DEGEL-projektet, inom ramen för detta projekt och även inom arbetet med MSBs lägescentral har det tydligt framkommit en rad svårigheter. Dessa beror på att personer inte känner varandra, att man kommer från olika organisationer eller från olika kulturer inom samma organisation. Normalt sett tar det tid att få personer inom eller mellan organisationer att ens lita på varandra – först behöver man träffas i jobbet kontinuerligt och på fritiden under mer sociala förhållanden. Trenden nu är att med den nya teknikens förmågor kunna föra samman människor som har lika intressen och som därmed kan ha samma mål. Hittar man gemensamma beröringspunkter i intressen utöver den professionella kontakten blir det betydligt enklare att samarbeta och därmed dela med sig av information.

Den ökande användningen av t.ex. Facebook och Twitter där man skapar sig en egen personlig nyhetssida som består av de egna vännernas nyheter medger även att spontana samverkansgrupper skapas vid kriser där information delas. Varje persons nyheter består av korta kommentarer (mikrobloggar), bilder, länkar, filmer, GPS-positioner m.m. På detta sätt får man en kontinuerligt uppdaterad lägesbild. Om denna typ av funktionalitet skulle användas dagligen av myndigheter och aktörer inom krishantering skulle detta skapa stora möjligheter att öka samverkan inom samhällets olika typer av stuprör. Facebook fungerar idag som en katalysator som för samman människor både privat och professionellt. Behoven som projektgruppen har upptäckt är att man inte vill samverka via öppna verktyg såsom Facebook utan via säkra lösningar som man har egen kontroll över – samtidigt som man vill utnyttja de befintliga nätverken och sociala verktygen som dominerar nu.



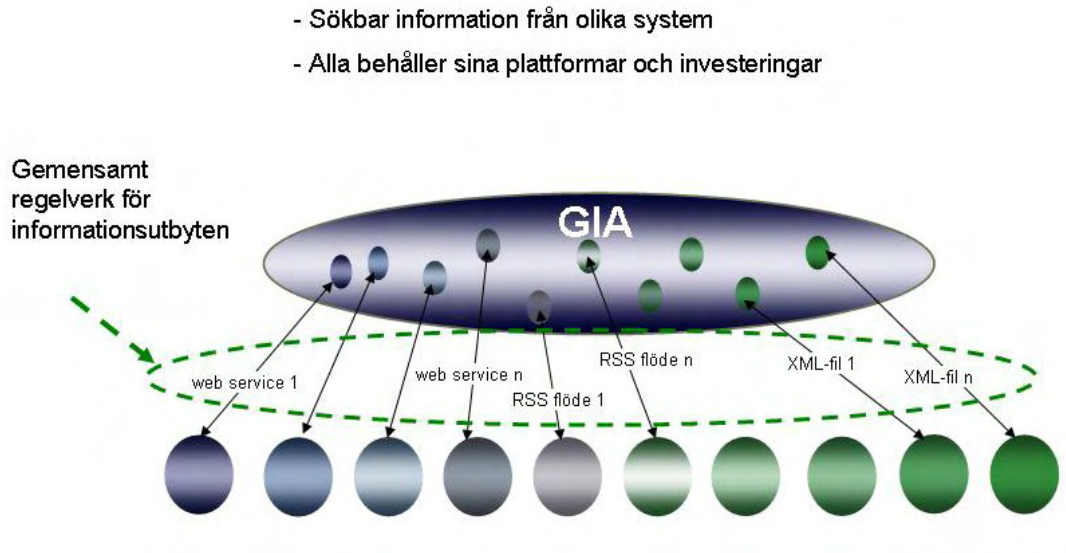
Figur 9: Secure Social Web för samverkansgrupper

Behovsanalysen pekar på tydliga trender som visar på en radikal ändring i användandet av mobiltelefoner. Det är främst företaget Apple och märket iPhone som har lett utvecklingen och under 2010 kommer alla stora telefonmärken att ha iPhone-liknande produkter. Effekten av att ha en stor skärm och att använda zoomningsteknik gör att människor använder telefonerna till fullo. Att använda öppna gränssnitt och erbjuda tredjepartsmarknaden en möjlighet att bidra med komponenter och idéer skapar konkurrens och ger lägre priser för användarna. I januari 2010 hade

över tre miljarder applikationer hämtats hem från Apple Store för iPhone-telefoner och de övriga tillverkarna har liknande marknadsplatser på gång.

Användningen av mobiltelefoner utöver ringandet består av att läsa nyheter från tidningar, skriva/läsa från sociala webben (Facebook m.fl.), ta fotografier och ta emot fotografier, använda kartor (navigering, skattletning, se var andra befinner sig m.m.), övervaka hälsa/motion, spela spel, lyssna på musik etc. Användningen av Internet i mobiltelefonerna gör att tjänster på nätet blir nätcentriska. Användarna kan påbörja en aktivitet vid datorn och fortsätta med den med hjälp av mobiltelefonen. Projektgruppen ser stora möjligheter att utveckla koncept och tjänster inom detta område i en nära framtid – problemet är mognad hos användare, beställare och investerare.

För att kunna dela information mellan organisationer och myndigheter (även inom stora organisationer) kontinuerligt behöver man ett systematiskt sätt att utbyta information. Genom att kapsla in information i ett XML(eXtensible Markup Language)-format Simple Information Sharing (SIS) kan man tillåta prenumeration och delning av information programmeringsmässigt på samma sätt som en leverantör av nyheter kan dela information till andra genom RSS (Really Simple Syndication). Med hjälp av en GIA-tjänst som söker efter och kan ta emot registreringar av rapportflöden kan man sammanställa relevant information som är klassificerad och strukturerad. GIA är tänkt att vara en tjänst som tillhandahåller länkar till information av specifik typ, t.ex. SIS. Genom att kapsla in data kan specifik information skrivas och läsas på ett generellt och programmeringsmässigt sätt.



Figur 10: Virtuell GIA för systematisk informationsdelning

På sikt kommer man att kunna registrera olika typer av informationstjänster och även mappnings-tjänster som nu t.ex. kan göras i integrationsverktyg såsom BizTalk, nServiceBus etc. Avsikten är att det ska kunna göras webbaserat och i en säker miljö.

Projektgruppen har även sett behoven av att potentiella kunder vill prova på och verkligen få testköra systemet. Det är alltid en sak att presentera idéer via broschyrer och PowerPoint-presentationer men oftast en helt annan sak att verkligen provköra. Det är då de s.k. riktiga behoven kan upptäckas (eller skapas). Samtidigt har inte den s.k. krishanteringsmarknaden varit tillräckligt mogen för att industrin ska kunna göra de investeringar som krävs för att nå fram till tillräckligt generella och anpassningsbara produkter. Därför är det av stor vikt att en eller flera provdrifter körs igång under 2009/2010 med olika typer av användare. I verktygen kommer sedan idéer och koncept registreras och arbetas fram.

Konceptgenerering och pilotprojekt

Projektgruppen inriktar sig på fyra olika områden. Det gäller för samverkande organisationer (och för Saab) att i högsta möjliga mån veta om:

- Varandra personligen (Knowing each other)
- Varandras processer, arbetssätt, varandras kulturer och metodik (Knowing how-to)
- Omvärlden (Knowing the world)
- Ny teknik (Knowing technology)

För att kunna arbeta mot samma överordnade mål och kunna göra detta kontinuerligt (det dagliga fikarummet, det dagliga mötet eller den dagliga konferensen) behöver man utnyttja ny teknik som idag och i framtiden används civilt t.ex. den sociala webben.

Verktyg som stödjer ovan områden har identifierats. Tillsammans med myndigheter och kunder ger dessa möjligheter att skapa anpassade lägesbilder och att bilda sociala nätverk som underlättar samverkan, samarbete och samordning. Dessa verktyg finns nu realiserade och samlade i SMED.

Verktygen är:

- Generell kartmodul (Google Maps) som man kan redigera och skicka data till (t.ex. polygoner, punkter, infotexter och vägmarkeringar).
- GIA, i vilken man kan registrera en URL till en webb-service eller en URL till ett RSS-flöde. Informationen som webb-service levererar kan man sedan söka efter. Formatet för informationen som webb-service levererar är ett enkelt XML-format som vi kallar SIS.
- Rapportering – varje rapport har i dagligt bruk en eller flera dedikerade läsare. Införandet av informationskanaler där man istället skriver eller genererar rapporter till ett prenumererbart informationsflöde. Rapportens innehåll kapslas in i ett av fälten i SIS.
- Secure Social Web – utnyttjande av tjänst liknande Facebook kommer att öka användningen och att öka informationsutbytet mellan de aktörer som deltar i försöken. Secure Social Web innehåller mikrobloggar, diskussionsforum, blogg, samverkansgrupper, dokumenthantering och meddelanden. En Helpdesk-funktion/förslagslåda kommer även att införas.
- Standardverktyg som t.ex. chatt, FAQ, gemensamma kalendrar, mediearkiv, wiki, kontaktlistor kan köras igång i portalen.
- Anpassade sidor för mobiltelefoner med stor skärm (s.k. smartphones).

Uppnådda resultat

Projektgruppen har under året lyckats med att få fram en kravbild som har skapats av olika aktörer inom olika verksamheter och på olika nivåer – från operativ nivå till strategisk. Samtliga behov och krav indikerar att man bör förverkliga verktyg för att underlätta samarbete, samordning och samverkan mellan och inom organisationer. Det handlar inte lika mycket om krishantering utan mer om hantering av komplexa situationer i vardagen – Everyday Complexity Management.

Under 2009 har projektgruppen realiserat moduler för lägesbild, rapportering och informationsdelning och driftsatt portalen i en modern miljö. Under 2010 kommer samverkansgrupper att kunna skapas inom vitt skilda områden och verksamheter. För Lindholmen

Science Parks del kommer verktygen att testas inom delprojekten och för MSBs del kommer vi att kunna erbjuda provdrifter för t.ex. skapande av sociala nätverk för Tjänsteman i Beredskap (TiB).

De nya förmågorna som SMED erbjuder kommer att testas och provas skarpt av en rad olika aktörer. MSB kommer att kunna utvärdera och projekten i Lindholmen Science Park kommer att kunna nyttja ”arenan” SMED under årets gång. Tillgången till de nya förmågorna gör att MSB och Lindholmen Science Park kan ligga i framkant vad gäller arbetssätt och medvetenhet kring vad nya sociala trender och ny teknik kan göra för att i slutändan infria målsättningar. Genom samverkan, samordning och samarbete kan alla parter nå sina mål.

Spridning av resultat

Arbetet inom projektet IFM har genererat ett antal publikationer och presentationer. Nedan beskrivs några av dessa:

- Euro-Atlantic Stakeholders Conference 2009 (EASC09) genomfördes den 1-2 oktober i Stockholm. Under denna konferens genomfördes två presentationer med anknytning till Security Arena. Den första, med titeln Increasing Resource Efficiency by Detecting Deviations in Information, hade anknytning till tidigare arbete inom SEPO-projektet och behandlade avvikande beteende i landbaserad transport. Den andra presentationen, med titeln Intelligent Surveillance Networks – Dynamic Integration of Sensors, Functions and Services, hade direkt anknytning till Delprojekt 1 av IFM.

- ITS World Congress 2009 genomfördes den 21-25 september i Stockholm. Till denna konferens accepterades ett papper med titeln Increased Transportation Security by Using Automatic Detection of Anomalous Truck Behaviour. En presentation genomfördes och fokus låg på tidigare arbete inom avvikelsedetektering i landbaserad transport.

- Den 17 september 2009 genomfördes ett uppskattat lunchseminarium, med titeln NIVS (Networked Intelligent Video Surveillance). Seminariet genomfördes i Security Lab och fokuserade på en del i ISN-konceptet (DP1) som rör videoövervakning. Seminariet var en följd av det tidigare projektet VARNA som genomfördes 2008 på Security Arena.

Inriktning 2010

Grundtanken under 2010 är att fortsätta att arbeta inom IFM och fokusera på att använda och utöka konceptet med GIA. Delprojekten Intelligent Surveillance Network, Information Management och Situation Awareness kommer drivas vidare med olika omfattning. Även nya projekt inom temat Surveillance and Early Warning planeras.

En vidareutveckling av befintliga projekt kan se ut som följer:

Delprojekt 1: Intelligent Surveillance Network

- Integrering av heterogena sensorer – fördjupa behovsanalysen och undersöka vad andra sensorer än kameror och radarer kan bidra med för nya förmågor.

- Datadriven anomalidetektering – årets pilotprojekt inkluderade regelbaserad anomalidetektering. År 2010 går vi vidare och studerar hur datadrivna (självlärande) metoder för anomalidetektering kan bidra till en ökad situationsförståelse under olika övervakningsuppdrag.

- Operatörsgränssnitt – tillsammans med användare diskutera hur ett operatörsgränssnitt (HMI) bör utformas och hur det skall kunna styras på ett enkelt och effektivt sätt.

Delprojekt 2: Information Management

För åren 2010-2012 är delprojektets inriktning att ta fram ett koncept för informationshantering, som ska inkludera frågeställningar och lösningar som berör informationssäkerhet. Konceptet ska utvecklas och tillämpas i samverkan Volvo Technology, akademin och Delprojekt 3 samt intressenter och myndigheter inom logistikdomänen.

Delprojekt 3: Situation Awareness

Under 2010 kommer arbetet att inriktas på att fortsätta realisera och utprova verktyg för bättre samverkan, samordning och samarbete mellan och inom organisationer med ansvar för krishantering och samhällssäkerhet.

Genom att väcka frågor och påvisa brister inom samverkansområden och samtidigt lyckas med att skarpt föra aktörer närmare varandra kan vidare ansträngningar och investeringar motiveras. Strävan att nå resultat i praktiken ska vara drivande, även om inblandade parter kanske endast samverkar under övningsförhållanden.

Situation Awareness och förmågor för att skapa förnuft i den totala datamängden kommer att vara central. GIA kommer att kunna byggas ut och testas i praktiken. Vi kommer att sätta igång arbetet med att ta fram förslag på hur ett regelverk för informationsutbyte mellan myndigheter skulle kunna fungera. För användargränssnitten i SMED gäller det att skapa s.k. "röda knappar" som användare inte kommer att kunna låta bli att trycka på - användarvänligheten ska ligga i fokus. Detta gäller även förmågor som ökar tillgängligheten i den driftsatta lösningen SMED. Aktörer ska kunna lämna information via mobiltelefoni (smartphones med lite större skärm).

I arenan SMED kommer det konkret att finnas funktioner för rapportering, karta, kommunikation och byggandet av sociala nätverk. Genom att införa GIA och ta med externa informationslämnare kommer data att kunna rapporteras eller samlas in och sedan bli sökbar via definierade och klassificerade informationskanaler.

Den feedback som projekten kommer att få i verktygen kommer vara styrande för utveckling av framtida arbetssätt inom olika samverkansområden i samhället. Dessutom kommer MSB direkt att kunna utvärdera vissa av verktygen under våren/sommaren 2010.

Tema 4: Metoder och system för robust och säker krishantering

Detta avsnitt beskriver verksamheten för temat Metoder och system för robust och säker krishantering inom Security Arena under år 2009. Inom ramen för temat har huvudsakligen bedrivits forskningsverksamhet.

Forskningens huvudmålsättning har inriktats mot metoder för att långsiktigt skapa en robust och säker infrastruktur för krisberedskapen och har skett i samverkan med de industriella aktörerna. Den har bedrivits inom ramen för fem delprojekt, som vart och ett behandlar viktiga aspekter av denna målsättning:

- Delprojekt 1: Intelligent säkerhetsloggning och nätövervakning
  Vi har undersökt effektiva sätt att genomföra datainsamling i övervaknings- och detekteringssyfte samt även utrett vilka krav som ställs för att datainsamlingen ska vara användbar för legala ändamål.

- Delprojekt 2: Tillförlitliga och robusta överföringsprotokoll – försvar mot tillgänglighetsattacker
  Vi har studerat metoder för att avvärja tillgänglighetsattacker mot webbapplikationer.

- Delprojekt 3: Kvantitativ modellering och utvärdering av säkerhet
  Problemet att kvantitativt kunna uppskatta säkerhet och säkerhetsförbättringar har studerats. Detta ger oss möjlighet att göra en avvägning mellan säkerhet och exempelvis ekonomiska aspekter.

- Delprojekt 4: Interaktiva beslutsstödssystem
  I detta delprojekt studerar vi beslutsstödssystem och möjliga framtida utformningar av sådana system som kan passa en civil myndighet med många aktörer.

- Delprojekt 5: Säker och självstabiliserad klocksynkronisering i sensornätverk
  Användning av sensornätverk för krisberedskapsändamål och studier av dessas säkerhetsbrister har genomförts.

Delprojekt 1 har fokuserat på hur man kan reducera mängden loggdata som samlas in, utan att för den skull ge avkall på kravet att man ur dessa data skall kunna extrahera relevant information. Forskningen har bedrivits med inriktning på loggmekanismer för intrångsdetekteringssystem, men är tillämpbar på många andra system, såsom exempelvis krishanteringssystem. Inom delprojektet har Ulf E. Larson framgångsrikt har försvarat sin doktorsavhandling On Adapting Data Collection to Intrusion Detection. Dessutom försvarade Magnus Almgren sin avhandling Techniques for Improving Intrusion Detection under december 2008. I och med detta har mycket väsentliga bidrag lämnats till forskningen inom området.

För delprojekt 2 har forskningen inriktats mot hur man kan mildra eller förhindra distribuerade tillgänglighetsattacker (Distributed Denial-of-Service - DDoS). Utöver försvaret mot primära attackmekanismer har vi även undersökt hur man kan försvara sig mot vissa sekundära attackmekanismer (Denial-of-Capability - DoC).

Arbetet inom delprojekt 3 har framskridit så långt att resultaten kommer att presenteras i form av en licentiatavhandling under första halvåret 2010. I avhandlingen beskrivs en systematik för området säkerhetsmetrik, vilken mottagits positivt inom forskarsamhället. Dessutom analyseras och värderas svårigheterna med att mäta säkerhet ur olika aspekter. Projektet skulle dock kunna ta ytterligare ett väsentligt kliv framåt om vi kunde få tillgång till autentiska data för vår säkerhetsmodellering. Detta har dock hittills visat sig vara svårt att åstadkomma.

Inom delprojekt 4 har vi med hjälp av intervjuer kartlagt hur krishanteringsverksamheten fungerat i några konkreta fall. Vi arbetar nu vidare med att dra slutsatser av detta material. Inom detta delprojekt gör vi även en utvärdering av ett koncept för ett s.k. interaktivt bord, med såväl fast som mobilt gränssnitt, för att utröna dess användbarhet och utvecklingspotential i krishanterings-sammanhang.

Inom delprojekt 5 har vi främst beforskat säker och robust gruppkommunikation för sensornätverk. Vi har inom delprojektet haft ett fruktbart samarbete med Saab.

Ett stort antal rapporter, publikationer och examensarbeten har producerats. Ytterligare examens-arbeten har påbörjats. Vi har haft en omfattande utåtriktad verksamhet, innefattande seminarier, kurser och kontakter med andra forskare och forskningsprojekt inom närliggande områden. Vi har exempelvis varit huvudansvariga för Security Arenas seminarieserie. Förutom den rent vetenskap-liga delen med konferenser med granskningsförfarande, träffar vi också många avnämare. I vår kurs i grundläggande datasäkerhet belyser vi olika aspekter av samhällssäkerhet och krishante-ring. Vi har vidare utökat vårt samarbete med Göteborgs universitet inom området samhällssäker-het (Societal Security). Det finns preliminära planer på att starta en masterskurs inom detta område.

En av gruppens medlemmar, Philippas Tsigas, har blivit utnämnd till professor vid Chalmers. Philippas kommer att fortsätta intressera sig för problem inom samhällssäkerhet och krisberedskap och utnämningen kommer därför att ge ett långsiktigt genomslag i forskarsamhället. Den visar dessutom indirekt på kvalitén av den forskning som har bedrivits inom projektet.

Vi har medverkat i en workshop och ett antal dedicerade möten med representanter för MSBs lägescentral, vilket varit givande för båda parter. Vi kunde lyfta ut en del av den forskning som vi utför och visa på dess relevans för de problem som en lägescentral ställs inför.

Slutligen noterar vi att projektets deltagare är aktiva medlemmar i den internationella forsknings-miljön och deltar i programkommittéer, konferenser, paneler och andra vetenskapligt relevanta konstellationer samt att vi blivit inbjudna att deltaga i ett antal EU-ansökningar inom ämnesområdet skydd av kritisk infrastruktur och samhällssäkerhet.

Delprojekt 1: Intelligent säkerhetsloggning och nätövervakning

Ulf Larson har framgångsrikt försvarat sin avhandling On Adapting Data Collection to Intrusion Detection. Avhandlingen behandlar hur man kan reducera mängden loggdata som samlas in och hur man underlättar besluten angående vilka loggmekanismer som ska användas vid olika tillfällen. I avhandlingen har detta problem studerats med avseende på intrångsdetektering, men de

utvecklade principerna har en allmän tillämplighet och skulle exempelvis kunna användas för den information som strömmar in till en ledningscentral. Dessutom har en modell för s.k. adaptiv loggning utvecklats. Denna modell beskriver hur loggar automatiskt kan slås av och på vid behov, vilket verksamt bidrar till effektiviteten.

Tomas Olovsson, tillsammans med masterstudenterna Sheikh Mahbub Habib och Cyril Jakob, har undersökt stabiliteten och säkerheten hos moderna avancerade smartphones eller vanliga telefoner vid avancerad användning, med till exempel en WiFi-uppkoppling. Deras resultat visar att många telefoner har stora säkerhetsbrister och en angripare kan lätt återstarta eller låsa en telefon genom enkla attacker. Arbetet har lett till flera publikationer och väckte också industriell uppmärksamhet. Tomas Olovsson har fått förfrågan från företag om detaljer om projektet. En av studenterna sökte och blev antagen som doktorand i Tyskland. Vi hoppas att vi fortfarande kan knyta an till hans arbete med detta projekt. För tillfället planeras inga vidare försök utan vi avvaktar återkoppling från industrin innan vi arbetar vidare med projektet.

Delprojekt 2: Tillförlitliga och robusta överföringsprotokoll

Flera olika parallella spår har följts i detta delprojekt. I ett av dessa har Zhang Fu koncentrerat sig på risker och hotbilder relaterade till öppna applikationer, som till exempel s.k. peer-to-peer-nätverk och sociala nätverk med distribuerade applikationer. Särskild hänsyn har tagits till effektivitetsaspekter, vilka vi har diskuterat i olika vetenskapliga fora. En annan aspekt som studerats är hur kraftfull en angripare måste vara för att kunna forcera det skydd som tidigare utvecklats inom detta projekt. Detta ger oss ett kvalitetsmått på hur bra lösningen är.

Zhang Fu har i samarbete med Marina Papatriantafilou studerat hur man kan mildra effekterna av distribuerade tillgänglighetsattacker (DDoS - Distributed-Denial-of-Service) genom att fokusera på distribuerad kontroll och teknisk enkelhet, vilket gör att metoden är praktiskt implementerbar. Redan föreslagna metoder använder antingen en centraliserad lösning som tyvärr inte är särskilt effektiv mot en attack som i sig själv är distribuerad, eller utnyttjar speciella s.k. tokens, som är svåra att använda i praktiken, eftersom de kräver en ”virtuell sluten krets”. I samband med denna studie sammanställer en examensarbetare strukturella egenskaper hos peer-to-peer-nätverk och data som kan användas för att prova nya metoders effektivitet.

Tillgänglighetsattacker har ofta sekundära effekter, dvs förutom det direkta målet för attacken störs också annan legitim trafik när den tillgängliga bandbredden minskar. Vi har föreslagit en proaktiv och klusterbaserad metod för att minska de skadliga effekterna. I denna balanseras effektiviteten mot den extra overhead av trafik som behövs. Metoden är kompatibel med olika s.k routing policies på nätverksnivå. Vi har estimerat metodens effektivitet och kommer att designa ett experiment för att direkt utvärdera algoritmen. Vi har också tagit fram en algoritm med vars hjälp man kan förbättra metoder som utnyttjar tokens för att framhäva legitim trafik. Vår algoritm minskar effekten av en särskild form av attack (DoC - Denial-of-Capability). På detta sätt förhindras komprometterade servrar i en domän att störa legitima servrar i en annan domän. Dessutom kan en legitim server i en domän med infekterade datorer garanteras service med en viss sannolikhet.

I de senaste forskningsresultaten angående robust kommunikation försöker vi också ta hänsyn till olika noders (användares) krav på tillit, tidigare kontakter, resurstillgång etc. S.k. overlays som kan tillgodose sådana krav kan lätt forma en grundstruktur av ett generellt peer-to-peer eller socialt nätverk med olika slags distribuerade applikationer.

I samarbete med en industripartner planerar vi att även beforska robusta ad-hoc nätverk och hur man där åstadkommer effektiv kommunikation även vid användning av mobila enheter, såsom mobiltelefoner eller rörliga fordon. Sådana nätverk kan tänkas komma till användning i ett flertal scenarier relaterade till samhällssäkerhet.

Delprojekt 3: Kvantitativ modellering och utvärdering av säkerhet

Vilhelm Verendel har arbetat med problematiken kring att utvärdera hur säkerhet fungerar och möjligheten att uttrycka detta kvantitativt. Detta görs dels ur ett systemperspektiv som innefattar teknik, beslutsfattande för säkerhet och behovet av ekonomisk riskmodellering. Målet har varit att modellera säkerhet som en egenskap som kan förstås i termer av exempelvis ekonomiska eller tekniska avvägningar. Vi har studerat olika vetenskapliga metoder, dels från traditionell feltolerans för tekniska system, dels från riskuppskattningar och beslutsfattande under osäkerhet från forskningen inom ekonomisk riskhantering. En bred studie av litteraturen inom säkerhets- och riskhantering har gjorts, vilken visar att det ännu inte finns några väletablerade metoder (baserad på empiri och beprövad erfarenhet) att se på säkerhet som en process som kan utvärderas exakt och kvantitativt. Resultat av denna studie har presenterats på en workshop.[24] Vidare har vi studerat ekonomisk modellering för att förstå beslutsfattares dilemman i säkerhet (till exempel i nätverk eller på företag) samt förutsägbara brister i beslutsfattande som kan modelleras på ett kvantitativt sätt. Vi har även undersökt möjligheten till konkreta metriker för tillgänglighet i komplexa nätverk.

Verksamheten har delvis hämmats av att vi skulle behöva få tillgång till autentiska data av något slag för vår modellering. Detta har visat sig vara svårt att åstadkomma, främst på grund av de integritetsproblem som spridning av data ger upphov till.

Två spår är i nuläget lovande för vidare forskning. För det första, kvantitativa mått på robusthet i nätverkstopologier (t.ex. elektroniska kommunikationsnätverk och sociala nätverk i krishantering). Här handlar det om hur olika mätetal kan vägas mot varandra när man designar komplexa nätverk som ska motstå angrepp. För det andra, riskmodellering av säkerhetsbeslut vad gäller beslutsunderlag för investeringar. Här kan man undersöka de modeller som tidigare utvecklats med hjälp av empiriska metoder, men i en simulerad situation. En artikel om detta har nyligen skickats till en workshop.[25]

Slutligen har vi knutit kontakter med representanter för EU-projektet AMBER, som är inriktat mot olika typer av metriker. Vi avser att söka etablera ett mer konkret samarbete i framtiden.

Delprojekt 4: Interaktiva beslutsstödssystem

Inom delprojekt 4 undersöks hur man kan förbättra och effektivisera beslutsstödssystem. Beslutsstödssystemen har till uppgift att tillhandahålla relevant och anpassad information till sina användare, både ur ett tekniskt och konceptuellt perspektiv.

Anna Gryszkiewicz har börjat kartlägga de generiska karakteristika som ett interaktivt beslutsstödssystem bör ha. Hon deltog i konferensen ISCRAM 2009 och även i Vad kan Sverige lära av kriser? i Stockholm i september (organiserat av MSB). En styrka med denna konferens var paneldebatterna med intressanta talare samt att deltagarna kom från vitt skilda sektorer i samhället. Ett föredrag diskuterade klimatförändringar och vad man kan och inte kan förvänta sig inom detta område. Inom konferensens ramar diskuterades flera olika problem, t.ex. problemet med dricksvatten, vilket väl stämde in på det arbete Anna har utfört tillsammans med en masterstudent. Detta arbete är nästan slutfört och kommer att utgöra grund för en vetenskaplig artikel.

Under hösten 2008 genomförde Anna fallstudier för att dokumentera och undersöka förloppet för två mindre krishändelser i Göteborgsområdet. Det ena fallet berörde de översvämningar som skedde i Mölndal i december 2006. Det andra fallet berörde ett smittoutbrott i dricksvattnet i Lilla

---

[24] V. Verendel, ”Quantified Security is a Weak Hypothesis”, New Security Paradigms Workshop, Oxford, UK, 8-11 September 2009

[25] V. Verendel, ”The Security Gap: Bias for Quantified Risk”

Edet hösten 2009. Syftet med fallstudierna var att studera hur information hanteras under praktiskt krisarbete hos olika aktörer. Fallstudierna fungerade som inspiration till en längre intervjuserie med olika krisaktörer i Sverige. Semistrukturerade intervjuer användes för att få veta mer om exakt vilka slags system som används för informationsinhämtning, bearbetning och spridning mellan olika aktörer. Intervjusvaren har använts för att bättre förstå vilka krav som ställs på stödsystem för informationshantering. Arbetet har nu resulterat i en rapport, som accepterats för publicering.[26] Tillsammans med en grupp examensarbetare har Anna även gjort en utvärdering av existerande svenska och internationella stödsystem för informationshantering, vilket har lett till ytterligare en publikation.[27] Anna har under våren 2009 gått MSBs grundkurs i krisberedskap. Slutligen har två masterstudenter arbetat vidare med sitt examensarbete inom ramen för detta projekt. Utifrån ett användarfokus ska de skapa och utvärdera en prototyp av beslutstödssystem för en lägescentral för krishantering.

Fang Chen har besökt Tsinghua University i Beijing, Kina och då speciellt avdelningen för Center of Public Safety Research. Detta framstående universitet har mycket bred erfarenhet av frågor som är centrala för krishanteringssystemet. Fang Chen undersöker nu möjligheten att närmare samarbeta med Tsinghua University, med fokus på ett utbyte av data för att bättre kunna lära sig av kriser. Ytterligare ett studiebesök på Tsinghua University med flera intresserade grupper planeras. Vidare finns långt framskridna planer på ett EU-projekt i samarbete med detta universitet. Ytterligare två projekt diskuteras. I det första studeras hur kulturella skillnader kan påverka designen av krishanteringssystem, medan man i det andra utnyttjar datorspel dels för att testa krishanteringssystemen och dels för att träna samverkan mellan dess aktörer. Vi har även fortsatt att odla våra kontakter med University of Chinnai, som drabbades av en tsunami 2004. Även här siktar vi mot ett framtida närmare samarbete och informationsutbyte.

Utveckling av MSBs lägescentraler i Karlstad och Stockholm

Magnus Almgren har, tillsammans med Marina Papatriantafilou och Morten Fjeld, arbetat med en studie med inriktning mot MSBs parallella lägescentraler, placerade i Karlstad och Stockholm, respektive. Detta arbete presenterades i september i samband med en workshop vid Security Arena, som helt allmänt handlade om lägescentraler för MSB. Magnus Almgren och Marina Papatriantafilou har deltagit i studiebesök vid MSBs lägescentraler i Karlstad och Stockholm. Marina, Magnus och Morten presenterade sedan viktiga forskningsresultat vid workshopen vid Lindholmen Science Park 3–4 september. Detta ledde till en ingående diskussion, där det framkom att MSB har intresse av både direkta studier och mer långsiktiga projekt.

Vi vill särskilt belysa den del av arbetet som Morten Fjeld, i samarbete med bland annat ETH i Zürich, har utfört inom CollaBoard-projektet. Collaboard är ett koncept för att presentera information för både samlokaliserade och avlägsna aktörer. Utrustningen består av två parallella whiteboards som är elektroniskt sammankopplade och speciellt anpassade för att skapa närvaro-känsla mellan gruppmedlemmar som samarbetar i geografiskt skilda lokaler, exempelvis i två parallella lägescentraler. En utvärdering har utförts och resultatet har sammanställts. Bland Mortens framtida planer ingår att just mäta hur väl gruppmedlemmarna kan samarbeta trots att de inte är på samma plats. En fortsättning av dessa studier diskuteras för närvarande med represen-tanter för MSB.

---

[26] Gryszkiewicz, A., Chen, F, Design requirements for information sharing in a crisis management command center, 7th International Conference on Information Systems for Crisis Respone and Management, ISCRAM 2010, May 2 to May 5, Seattle, Washington, USA, 2010.

[27] Oduor, E., Nihal. P., Gryszkiewicz, A., Chen, F, Concept for intelligent integrated system for crisis management, 7th International Conference on Information Systems for Crisis Respone and Management, ISCRAM 2010, May 2 to May 5, Seattle, Washington, USA, 2010.

Delprojekt 5: Säker och självstabiliserad klocksynkronisering i sensornätverk

Fokus i detta delprojekt har varit att beforska säkra och robusta protokoll för sensornätverk. Säkerhet och robusthet är två väsentliga egenskaper för nätverk som ska arbeta i öppna miljöer, ofta utan uppsikt eller fysiska skyddsbarriärer. Andreas Larsson och Philippas Tsigas har utvecklat och presenterat den första algoritmen för säker och självstabiliserande klocksynkronisering för sensornätverk som är installerade i en speciellt utsatt miljö, där en angripare t.ex. kan ta över noder och fördröja meddelanden.

Enhetlig tidsuppfattning mellan noderna i ett sensornätverk är en viktig grund för flera andra funktioner i nätverket. Till exempel behövs noggrant synkroniserad tid, dels för att lokalisera och bestämma orsakssamband för händelser, dels för att kunna filtrera redundant information. Synkroniseringen behövs också för att kunna schemalägga radiotrafik med avsikt att minska störningar mellan noderna. En artikel om detta har presenterats vid konferensen the 9th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS '07) och en utökad artikel har skickats in till en vetenskaplig tidskrift. Inom detta område har Farnaz Moradi och Asrin Javaheri avslutat ett examensarbete med titeln Clock Synchronization in Sensor Networks for Civil Security.

Vi har även studerat hur gruppkommunikation i sensornätverk kan göras säker och robust. Precis som klocksynkronisering, så är gruppkommunikation en grundläggande service som behövs för att bygga andra mer abstrakta tjänster i nätverket. En sådan kommunikationsservice måste klara av den dynamiska topologi som används i sensornätverk och de speciella attacker som därmed kan riktas mot dem. Noder kan försvinna från nätverket om deras batteri tar slut eller om de går sönder, exempelvis på grund av en ogästvänlig omgivning. Dessutom tillkommer noder vid påfyllning av nätverket. Angripare kan också aktivt försöka påverka nätverket så att det mister sin funktionalitet eller ger missledande information. En uttömmande artikel om denna forskning har framtagits och skickats in till en tidskrift.

Under sommaren avslutades ett examensarbete av Lander Casado där han implementerade symmetrisk kryptering för sensornätverk, vilket presenterades vid NordSec 2009 i Oslo. Arbetet har resulterat i ett mycket viktigt steg för Contiki, det operativsystem för sensornätverk som Saab använder. Vi planerar nu ett nytt examensarbete för att även implementera asymmetrisk kryptering.

Vi har även undersökt vilka fördelar som kan ernås genom att kombinera kameradata med data från sensornätverk. Data från sensorer med passiva infraröda detektorer kan då användas tillsammans med video från kameror för att följa personer och föremål, vilket ger en tillförlitligare bild än vad bara videon kan göra. Bland annat förbättras möjligheten att spåra överlappande objekt. Vi hoppas att kunna fortsätta denna forskning i samarbete med Saab.

Samarbeten och synergier inom Security Arena

En styrka med Security Arena är synergieffekterna mellan akademi, industri och samhälle i den s.k. Triple Helix-strukturen som byggts upp. Det finns klara fördelar för forskningen att arbeta nära industrin, även om de grundläggande målsättningarna skiljer sig åt. Forskningen arbetar med idéer och koncept och siktar mot långsiktig kunskapsuppbyggnad medan industrin arbetar på att få fram produkter i ett många gånger mycket kortsiktigt perspektiv. Icke desto mindre är det av värde att forskningen får direkt inblick i problem som industrin och även myndigheter brottas med.

Genom examensarbeten har studenter fört ut de senaste resultaten till industriprojekt, och sedan fört med sig erfarenheter tillbaka till högskolan där de presenterat sina arbeten. Ett typiskt sådant exempel är beskrivet i detalj i anslutning till delprojekt 5. I ett flertal fall har studenterna sedan fått anställning hos de industriella parterna på arenan för att arbeta med de gemensamma projekten. Det finns också exempel på rekrytering motsatt riktning. En nyanställd doktorand på avdelningen arbetade innan hos en av våra industripartners. Även om denna nya doktorand inte direkt kommer

att arbeta inom Security Arena hoppas vi kunna utnyttja hans industriella erfarenheter. Vidare har de tematiserade projekten haft tillgång till forskare i sina expertgrupper. Förhoppningsvis har detta lett till en bättre genomlysning av de lösningar som valts.

Kunskapsspridning genom seminarieserie

Vår seminarieserie för att sprida våra och andras forskningsresultat till en bredare publik har fortsatt under 2009. Se Bilaga 1.

Dessa seminarier är ett utmärkt tillfälle för forskningsdelen på Security Arena att kommunicera resultat till industrideltagarna, men också till en bredare publik eftersom dessa seminarier är öppna för alla som har intresse av IT och samhällssäkerhet. Ett tillfälle utnyttjades till att låta en person från MSB komma och föredraga om RAKEL, eftersom det hade stort intresse för deltagarna på Security Arena samt andra beslutsfattare och avnämare på regional nivå.

Specifika resultat

Arbetet inom forskningsprojektet har genererat ett stort antal publikationer och tekniska rapporter. Dessa listas i Bilaga 3.

Vidare har ett antal relevanta examensarbeten genomförts. Även dessa listas i Bilaga 3. Examensarbeten kan utgöra en naturlig brygga mellan forskningsprojekten och industriella projekt på Security Arena. Speciellt vill vi påpeka att flera nya examensarbeten använder den sensornätverksplattform som vi fick tillgång till genom samarbetet med Saab. Detta ger möjlighet att ha en gemensam plattform för provförsök och förenklar också spridningen av forskningsresultat till industrin. Ett annat exempel på samverkan är examensarbetet utfört av Davide Bozza, som binder ihop vår forskning med Saabs projekt VARNA.

Vi noterar också att projektets deltagare är aktiva medlemmar i den internationella forskningsmiljön och medverkar i programkommittéer, paneler, konferenser och andra vetenskapligt relevanta konstellationer. Dessa listas i Bilaga 4.

Annan verksamhet av intresse för MSB

Kursverksamhet

Forskningsgruppen ger ett flertal kurser med anknytning till våra projekt. Elad Schiller har handlett en kurs i sensornätverk vid Chalmers i vår. Kursen, Seminar on Algorithms for Sensor and Ad Hoc Networks ges främst för doktorander och mastersstudenter i slutet av sin utbildning. Philippas Tsigas har givit fortsättningen på förra årets doktorandkurs Research Topics in Security in the context of Crisis Management and Societal Security med inriktning mot forskning som är relevant för samhällssäkerhet.

Marina Papatriantafilou och Philippas Tsigas med flera organiserade MiNEMA Winter School 2009: the 2009 Winter School in Middleware for Network Eccentric and Mobile Applications i Göteborg 23–26 mars, 2009. Det var cirka 100 deltagare, däribland flera doktorander från vårt forskningsprojekt. Experter på nätverk för mobil kommunikation och middleware-system från hela Europa samlades och tillsammans med doktorander och andra unga lovande forskare diskuterade området. Förutom den breda kunskap som förmedlades gavs också möjligheter till ett extensivt nätverkande. För doktorander var denna vinterskola därmed ett utmärkt tillfälle att bygga framtida forskningsnätverk. Särskilt diskuterades utmaningen att identifiera nya programspråk, eller nya specialiseringar av redan kända språk, som också fungerar för mobila system och peer-to-peer-system. Detta område är sålunda en grundsten i förmågan att kunna kommunicera säkert, även om man bara har tillgång till ett mobilt system. Även industriella deltagare från Security Arena var inbjudna till denna vinterskola.

Flera doktorander och seniorer deltog vid den årliga sammankomsten för det svenska nätverket SWITS (The Swedish IT-Security Network for PhD students) i Karlskrona, Blekinge i juni. Andreas Larsson presenterade där sitt arbete med sensornätverk.

Under första delen av hösten undervisar också Erland Jonsson och Magnus Almgren masterstudenter i kursen Computer Security. I denna kurs medverkade även Vilhelm Verendel och Pierre Kleberger.

Samverkan med externa projekt

FORWARD är ett EU/FP7-projektet, som har hög relevans för vårt arbete inom Security Arena, i synnerhet den del som Erland Jonsson sammanhåller för Chalmers, nämligen arbetsgruppen för Kritiska system. FORWARD har helt allmänt i uppgift att kartlägga framtida allvarliga IT-relaterade hot och ett utkast av denna kartläggning presenterades för EU i Bryssel i februari. Chalmers bidrog med hot mot kritiska infrastrukturer. Utkastet omarbetades och presenterades på en workshop i Nice 4-5 maj 2009. Representanter från MSB deltog i workshopen och framförde värdefulla synpunkter. Sammanfattningsvis uppfattades kartläggningen som mycket relevant och det diskuterades i flera olika konstellationer hur man med denna kartläggning som grund kan gå vidare med mer konkreta projekt. Ett problem som speciellt diskuterades var den mänskliga faktorn. Trots att det är välkänt att tekniska system inte själva kan garantera säkerhet, utan att hänsyn också måste tas till den mänskliga faktorn (t.ex. i form av en trött operatör), sker lite forskning på området Användbar Säkerhet.

Ett nytt projekt har påbörjats som delvis bygger på det arbete som gjorts inom Security Arena. Doktoranden Farnaz Moradi har anställts för att forska om problemet med spam på Internet. Detta spam-projekt finansieras av stiftelsen för Internetinfrastruktur (.SE) och har redan rönt ett visst intresse från media.[28] Farnaz Moradi gjorde sitt examensarbete med sensornätverk inom ramen för Security Arena. Eftersom hon är väl så insatt i problematiken inom samhällssäkerhetsområdet hoppas vi på framtida synergieffekter mellan spam-projektet och Security Arena.

Andra ansökningar, som till exempel deltagande i ett Network of Excellence, har skickats in under hösten. I och med vårt arbete inom Security Arena har vi byggt upp en vetenskaplig expertis som efterfrågas av samarbetspartner i Europa när projekt eller nätverk byggs upp. Dessa ansökningar riktar sig både till EU/FP7 och till European Science Foundation.

---

[28] Se till exempel http://www.svd.se/naringsliv/nyheter/artikel_3501253.svd

Marina Papatriantafilou samarbetar också med Elad Schiller och Georgios Georgiadis i två projekt av intresse för MSB. I det första studeras bättre algoritmer för effektiv kommunikation i ad-hoc nätverk av mobila eller bilnätverk, t.ex. att etablera ett nytt nätverk i ett område vid kris. I den föreslagna algoritmen tas bättre hänsyn till att de mobila enheterna faktiskt inte är stationära. I arbetet med Georgios Georgiadis studerar Marina Papatriantafilou hur trafik bör skickas, baserat på tillit (eller liknande metriker) mellan noderna i moderna overlay-nätverk.

Samverkan med externa forskare

Vi har fördjupat vårt samarbete med externa forskargrupper. Robert Cunningham från Lincoln Labs, USA, höll ett seminarium med titeln Refining Security: Process Control System Protection, Misuse Detection and Attack Response. Han redogjorde för ett större projekt som de har i USA med att bygga bättre processkontrollsystem.

S. Felix Wu höll ett seminarium med titeln Davis' Social Netorks, där han presenterade viktiga detaljer nödvändiga för "nästa generation av Internet". Mer specifikt gick han in på hur man kan upprätta och skydda kombinerade sociala nätverk och datanätverk, samt den inbyggda tillit som finns i sådana nätverk.

Inriktningen av framtida forskning

Vår ambition är att fortsätta bedriva forskningen i stort sett i linje med våra nuvarande planer. Forskningen till sin natur är långsiktig och vi tror fortfarande att den inriktning som vi tidigare fastställt även i fortsättningen kommer att vara till gagn för MSB. Om man beaktar den aktuella och kända finansieringssituationen, så kommer fokus inom ett beviljat fortsättningsprojekt att inriktas på säkerhetsaspekter inom informationssystem och sensornätverk samt metoder att kvantitativt validera dessa.

Ett intressant område, där vi skulle vilja utöka vår forskning, är hur man kan förbättra, säkra och effektivisera arbetet i lägescentraler, bland annat med avseende på hur man samverkar mellan geografiskt skilda centraler.

Förkortningar och begrepp

ADR	Europa-gemensamt regelverk för transport av farligt gods på landsväg
Anomali	Avvikelse från normalmodell
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosives
DGD	Dangerous Goods Declaration
DEGEL	Demonstrator Gemensam Lägesbild
DHL	Företag inom expressfrakt och logistik
DPx	Delprojekt nr x
e^2Call	Extended eCall är en vidareutveckling av eCall projektet. e^2Call är anpassat för att möta tunga fordons behov i synnerhet i samband med farligt godstransporter
e2e	End-to-end
eCall	Ett initiativ ifrån Europeiska kommissionen, som syftar till snabba upp responstiden för olyckor som involverar motorfordon
EU/FP7	Framework Program number 7 inom EU
FAQ	Frequently Asked Question(s) är en samling ofta ställda frågor och deras svar
FMV	Försvarets Materielverk
FOI	Totalförsvarets forskningsinstitut
FORWARD	EU-projekt inom området ”Hot mot säkra infrastrukturer”
FRA	Försvarets Radioanstalt
GHN	Government Home Network, en kommunikationslösning som ger en myndighets-operatör kontroll över ett mobilnät och nyttjar andra operatörers radionät (liknande Halebop som nyttjar TeliaSoneras nät)
GIA	Gemensam InformationsArea
GIS	Geografiskt Informationssystem
GPRS	General Packet Radio Services
GPS	Global Positioning System
GRS	Group-Radio Solution
GSM	Groupe Spécial Mobile, globalt system för mobil kommunikation
IFM	Information Flow Management
IMDG	International Maritime Dangerous Goods Code
IMO	International Maritime Organization
ISN	Intelligent Surveillance Network
ITS	Intelligent Transport System
KBM	Krisberedskapsmyndigheten
KBV	Kustbevakningen
M2M	Machine-to-Machine
MSB	Myndigheten för Samhällsskydd och Beredskap
NATO	North Atlantic Treaty Organization
NEC	Network Enabled Capability
NIVS	Networkt Intelligent Video Surveillance
PMR	Private Mobile Radio
POC	Proof-of-Collection
POD	Proof-of-Delivery
PTS	Post- och telestyrelsen

PTT	Push-to-talk
PTZ	Pan-Tilt-Zoom
QuicLINK	Ett komplett och bärbart mini-3G-nät (Ericsson)
Quickwins	Benämning på ett tekniskt experiment
RAKEL	Radiokommunikation för effektiv ledning
RFID	Radio Frequency Identification är en teknik för att läsa information på avstånd från transpondrar och minnen som kallas för taggar
RID	Europa-gemensamt regelverk för transport av farligt gods på järnväg
RPS	Rikspolisstyrelsen
RSS	Really Simple Syndication
SAFER	Fordons och trafiksäkerhetscentrum
SEPO	Secure and Efficient Port Operations
SIMSEC	Ett namn på krypterad röstkommunikationsprodukt
SIRS	Saab Intelligent Radar Sensor
SIS	Simple Information Sharing
SMED	Sensemaking Engine Demonstrator
TAPA	Transported Asset Protection Association
TETRA	TErrestrial Trunked RAdio, mobiltelefonistandard med inbyggda specialfunktioner
3G	Tredje generationens mobiltelefonisystem
3GPP	3rd generation partnership project
URL	Uniform Resource Locator
VARNA	Video Analysis for Real-time Networked Awareness
Volatile	
Whiteboard	Programvara för tillfällig delning av känslig information
Wiki	En sökbar webbplats där sidorna kan redigeras av besökarna själva
XML	eXtended Markup Language

Bilaga 1: Kunskapsspridning genom seminarier och konferenser

Här listas de seminarier och konferenser som har genomförts i Security Arena under 2009.

Kunskapsspridning genom Security Arena lunchseminarieserie

Följande lunchseminarier har genomförts[29]:

- 19 mars: A defence-in-depth approach to securing the connected car
  Dennis Nilsson, Chalmers
- 23 april: Constructing robust and secure web applications
  Andrei Sabelfeld, Chalmers
- 25 juni: RAKEL: Status, tjänster och utbyggnadsplaner
  Leif Zetterberg, MSB
- 24 augusti: Socialt nätverk för krissituationer
  Vilhelm Verendel, Chalmers tekniska högskola
- 17 september: NIVS - Advanced Video Surveillance Communication
  Hans Åkerlund och Per Lindquist, Saab Bofors Dynamics AB
- 15 oktober: Log management and SIEMs – an overview
  Ulf Larson, Omegapoint
- 12 november: Göteborg region IT infrastructure – GREAT
  Birger Ekengren, GREAT
- 8 december, ICT as tools for peace building, crisis management and disaster recovery
  Dag Nielsen, ICT4Peace

Seminarier och konferenser för Tema 1: Samhällskritiska transporter

Representanter från Tema 1 har presenterat material vid följande seminarier och konferenser:

- Polisens transportsäkerhetsdag, Göteborg, 25 mars
  Presentation av arbetet med hot från organiserad brottslighet mot transportsektorn
- Transports logistics, München, 13-15 maj
  Presentation av Security Arena och arbetet med fokus på transporter av farligt gods
- Seminarium vid The Insurance Bureau Vehicle Crime (försäkringsbolag i Nederländerna), Nederländerna, 25 juni
  Presentation av arbetet med hot från organiserad brottslighet mot transportsektorn
- Workshop MSB lägesbild, Göteborg, 4 september
  Generell presentation av Tema 1

[29] Se http://www.lindholmen.se/sv/vad-vi-gor/security-arena/seminarier

- ITS World Congress, Stockholm, 21-25 september
  Presentation av pilotprojektet Säkra och effektiva transporter genom hamn 2008
  Fyra visningar av Demoteatern ”Secure Transports”

- Knowledge Sharing: Anti-Theft Security, internt seminarium för Volvogruppen, Göteborg, 29 september
  Presentation av arbetet med hot från organiserad brottslighet mot transportsektorn

- IRU (International Transport Union) möte med fokus på farligt gods, Köpenhamn, 2 oktober
  Presentation av Security Arena och arbetet med fokus på transporter av farligt gods

- Kommunal olyckskonferens, Göteborg, 11 november
  Presentation av arbetet relaterat till farligt gods

- 5th Seminar on the Fight against International Vehicle Theft, (Nätverkande mellan polis från EU-medlemsstater med syfte att effektivisera samarbetet och bekämpa organiserade fordonsstölder i Europa), Göteborg, 17 november
  Presentation av arbetet med hot från organiserad brottslighet mot transportsektorn

- Säkra godstransporter i centrala Göteborg, Mölndal, 26 november
  Presentation av arbetet med hot från organiserad brottslighet mot transportsektorn

- EUs generaldirektörer för civilskydd, Göteborg, 10 december
  Generell presentation av Tema 1

Bilaga 2: Expertgrupper för Security Arenas temaprojekt

Nedan listas medlemmarna i de olika expertgrupper som engagerats inom Security Arenas temaprojekt 2009.

Expertgruppen för Tema 1

Delprojekt 1: Demoteatern – Secure transports

Intervjuade organisationer och företag:

- Avsändare
  - AkzoNobel
- Intresseorganisationer
  - Sveriges Åkeriföretag
  - Sveriges Hamnar
- Rederier & hamnar
  - Cobelfret
  - DFDS Tor Line
  - Göteborgs Hamn
  - Stena Line
- Säkerhetsrådgivare & konsulter
  - Farligt Gods Center
  - RPG Group
  - Sten FG
- Speditörer
  - DHL
  - DSV
  - Schenker
- Myndigheter
  - Kustbevakningen
  - MSB
  - Polismyndigheten
  - Transportstyrelsen
- Åkerier
  - ADR-Hanape
  - Eriksson Åkeri
  - GJAB
  - Green Cargo
  - Hoyer

Delprojekt 2: Hot från organiserad brottslighet mot transportsektorn

Medlemmar i Transportsäkerhetsgruppen Göteborg:

An Paepen	Volvo Trucks
Anders Lomander	France Sped
Annika Persson	Sveriges Åkeriföretag
Björn Edsholm	Dagab Syd
Claes-Bertil Ohlsson	Securitas
David Hellsing	Tullverket
Erik Vilhelmsson	LFB
Eva-Lotta Leimalm	GTS
Fredrik Bode	Volvo Technology
Gilbert Mellin	GTS

Hans Fahlen	Länsförsäkringar
Henrik Petzäll	Trafikkontoret
Ingemar Nilson	Godsletaren Tracing
Jimmy Kroon	Mobile Consulting NSWE
Johan Lomander	Speedcargo
Johan Ohlsson	Securitas Maritime & Logistics
Jonas Böös	Komplett.se
Karl-Erik/Yvonne Andreasson	Andreassons Åkeri
Klas Wassberg	Guard Systems
Lars Hubinette	HML
Leif Enarsson	Göteborgs universitet, Handelshögskolan
Lennart Dahlback	DFDS Tor Line
Mats Rodin	Rodcon
Morgan Olausson	Kuhne-Nagel
Olle, G Bernstaf	DHL
Olof Ekman	Ekmans Åkeri Ödsmål
Patrik Grauers	DHL
Pelle Joelsson	Trygg-Hansa
Per Nilsson	MICCRO-RO
Per Arne Nilsson	Polisen
Peter Liljenfors	DSV Road AB
Pontus All	Volvo Technology
Robert Gårdsmed	DSV Road AB
Roger Klahr	Posten Logistik
Stefan Jakobsson	Nacora International Insurance Brokers
Stefan Törneberg	Transportarbetarförbundet
Sören Kullberg	If
Thomas Morell	Sveriges Åkeriföretag
Åke Dennås	Säkerhetsrådet
M.fl.	

Medlemmar i Säkra godstransporter i centrala Göteborg:

Bo Hermansson	Green Cargo
Fredrik Bode	Volvo Technology
Hans Ljungberg	Svensk Åkeriförening
Håkan Löwberg	Polisen
Lennart Jivegren	Posten
Magnus Jaderberg	Trafikkontoret
Marianne Sörling	Innerstaden Göteborg
Niclas Coster	Bring Express
Per Arne Nilsson	Polisen
Pontus All	Volvo Technology
Roger Nilsson	TGM (Schenker)

Expertgruppen för Tema 2

Ingen explicit expertgrupp är engagerad 2009.

Expertgrupper för Tema 3

Expertgruppen i delprojekt 1 omfattar följande medlemmar:

Thomas Fransson	Göteborgs hamn
Kristian Fred	Preem
Johan Ohlsson	Securitas
Peter Martin	Peab
Jan-Ivar Andersson	Tullverket
Dan Larsson	LFV Landvetter
Åke Söderberg	Got Event
Bengt-Arne Bom	Länsstyrelsen i Västra Götaland

Expertgruppen i delprojekt 2 omfattar följande medlemmar:

Leif Björklund	Larmtjänst
Jonas Broberg	Enköpings åkeri
Daniel Ekwall	Schenker /Chalmers
Per-Arne Nilsson	Polisen i Västra Götaland
Camilla Oscarsson	Enheten för farliga ämnen, MSB
Luca NGIL Urciuoli	Lunds Universitet

Expertgruppen i delprojekt 2 omfattar följande medlemmar:
Här anges endast organisationerna.

Länsstyrelsen i Kronoberg
Länsstyrelsen i Kalmar
Linköpings kommun
Tekniska Verken i Linköping AB
RPS
MSB

Expertgruppen för Tema 4

Ett verksamt forum för att åstadkomma synergier är samverkan inom ramen för expert- och referensgrupper. Expertgruppen för forskningen har till uppgift att ge råd och synpunkter på forskningens långsiktiga inriktning. Den omfattar följande medlemmar:

Åsa Boholm	Göteborgs universitet
Sigvard Brodén	Saab Group
Daniel Haglund	MSB
Ingvar Hellquist	MSB
Mikael Korhonen	MSB
Henrik Olofsson	TeliaSonera R&D
Johan Wagné	Ericsson
Vesa Virta	FRA

Representanter från Chalmers

Bilaga 3: Publikationer, rapporter och examensarbeten för Tema 4

I denna bilaga listas de publikationer och tekniska rapporter, som tagits fram inom ramen för Tema 4. Dessutom listas de examensarbeten, som handletts av forskare inom Security Arena och som är relevanta för MSB.

Publikationer

- Shlomi Dolev, Elad M. Schiller, Paul G. Spirakis, Philippas Tsigas, Strategies for Repeated Games with Subsystem Takeovers Implementable by Deterministic and Self-Stabilizing Automata, In Second International Conference on Autonomic Computing and Communication Systems. Also to appear in International Journal of Autonomous and Adaptive Communication, 2009.
- Niklas Elmqvist, Ulf Assarsson, Philippas Tsigas, Dynamic Transparency for 3D Visualization: Design and Evaluation", In International Journal of Virtual Reality, to appear, 2009.
- Daniel Cederman, Philippas Tsigas, GPU-Quicksort: A Practical Quicksort Algorithm for Graphics Processors, In the ACM Journal of Experimental Algorithmics (JEA), ACM press.
- Anders Gidenstam, Marina Papatriantafilou, Philippas Tsigas, NBmalloc: Allocating Memory in a Lock-Free Manner, In Algorithmica, Jan 2009. Springer
- Phuong Hoai Ha, Philippas Tsigas, Otto J. Anshus, Preliminary results on nb-feb, a synchronization primitive for parallel programming, PPOPP 2009: 295-296.
- Vilhelm Verendel, The Security Gap: Bias for quantified risk. Technical report
- Sheikh Mahbub Habib, Cyril Jacob and Tomas Olovsson: An Analysis of the Robustness and Stability of the Network Stack in Symbian-based Smart phones. Article to appear in Journal of Networks, SI of ICCIT'08, Volume 5, Number 1, January 2010
- Vilhelm Verendel: Quantified Security is a Weak Hypothesis, New Security Paradigms Workshop, Oxford, England, 8-11 September 2009
- Zhang Fu, Marina Papatriantafilou, Philippas Tsigas, Wei Wei: Mitigating Denial of Capability Attacks Using Sink Tree-Based Quota Allocation, submitted to 2010 ACM Applied Computing Conference (Networking track).
- Lander Casado, Philippas Tsigas: Secure Communication in Wireless Sensor Networks. In Workshop on Self-Organising Wireless Sensor and Communication Networks, 8 – 9 October 2009, Hamburg, Germany.
- Lander Casado, Philippas Tsigas: ContikiSec: A Secure Network Layer for Wireless Sensor Networks under the Contiki Operating System. In the Proceedings of the 14th Nordic Conference on Secure IT Systems (NordSec 2009), Lecture Notes in Computer Science Vol.: 5838, pages 133 - 147, Springer-Verlag 2009.
- Jaap-Henk Hoepman; Andreas Larsson; Elad Michael Schiller; Philippas Tsigas. Secure and Self-Stabilizing Clock Synchronization in Sensor Networks. Theoretical Computer Science (journal), Elsevier, special issue on Security and Self-Stabilization, Revised version submitted.
- Phuong Hoai Ha, Philippas Tsigas, Otto J. Anshus. The Synchronization Power of Coalesced Memory Accesses. IEEE Transactions on Parallel and Distributed Systems 2009.
- Phuong Hoai Ha, Philippas Tsigas, Otto Anshus. Preliminary results on NB-FEB, a synchronization primitive for parallel programming. In the Proceedings of the 14th ACM

SIGPLAN symposium on Principles and practice of parallel programming (PPoPP 2009), pages 295 - 296, ACM press 2009.

- Phuong Hoai Ha, Philippas Tsigas, Otto Anshus. NB-FEB: A Universal Scalable Easy-to-Use Synchronization Primitive for Many core Architectures. In the Proceedings of the 13th International Conference of Distributed Systems (OPODIS '09).
- Pierre Leone, Marina Papatriantafilou, Elad Schiller; Relocation Analysis of Stabilizing MAC Algorithms for Large-Scale Mobile Ad Hoc Networks, Algosensors 2009: 5th International Workshop on Algorithmic Aspects of Wireless Sensor Networks, July 2009, LNCS, Springer Verlag.
- Pierre Leone, Marina Papatriantafilou, Elad Schiller, Mobility Models and Stabilizing MAC Algorithms for Mobile Ad Hoc Networks; Accepted as short paper in SSS 2009, 11th International Symposium on Stabilization, Safety, and Security of Distributed Systems, LNCS series, Springer Verlag.
- Georgios Georgiadis and Marina Papatriantafilou : A Least-Resistance Path in Reasoning about Unstructured Overlay Networks, The 15th International European Conference on Parallel and Distributed Computing (Euro-Par 2009); distinguished paper award; August 2009, LNCS, Springer Verlag.
- Pierre Leone, Marina Papatriantafilou, Elad M. Schiller and Gongxi Zhu: Analyzing Protocols for Media Access Control in Large-Scale Mobile Ad Hoc Networks, accepted in the Workshop for Self-Organising Wireless Sensor and Communication Networks, October 2009, (ISBN to appear).
- Shlomi Dolev, Elad Michael Schiller, Paul Spirakis, Philippas Tsigas: Strategies for Repeated Games with Subsystem Takeovers Implementable by Deterministic and Self-Stabilizing Automata. In International Journal of Autonomous and Adaptive Communication (special issue devoted to selected papers of the 2008 Second International Conference on Autonomic Computing and Communication Systems.
- Gryszkiewicz, A., Chen, F., 2010, Design requirements for information sharing in a crisis management command center, 7th International Conference on Information Systems for Crisis Respone and Management, ISCRAM 2010, May 2 to May 5, Seattle, Washington, USA (to appear).
- Oduor, E., Nihal. P., Gryszkiewicz, A., Chen, F., 2010, Concept for intelligent integrated system for crisis management, 7th International Conference on Information Systems for Crisis Respone and Management, ISCRAM 2010, May 2 to May 5, Seattle, Washington, USA, (to appear).

Tekniska rapporter

- Vilhelm Verendel: The Security Gap: Bias for quantified risk, TR Department of Computer Science and Engineering, Chalmers University of Technology, 2009, (submitted to Financial Cryptography 2010).
- Zhang Fu. Marina Papatriantafilou, Philippas Tsigas CluB: A Cluster Based Method for Mitigating Distributed Denial of Service Attacks. Technical Report (to appear).
- Zhang Fu, Marina Papatriantafilou, Philippas Tsigas, Wei Wei: Protecting Against Denial of Capability Attacks Using Sink Tree-Based Quota Allocation, TR Department of Computer Science and Engineering, Chalmers University of Technology, 2009.
- Georgios Georgiadis and Marina Papatriantafilou: Overlays with preferences: Approximation algorithms for matching with preference lists. TR Department of Computer Science and Engineering, Chalmers University of Technology, 2009.

Examensarbeten

- David Holmin, Methods for Exploiting Function-Level Parallelism in OpenMP 3.0.
- Muhammad Tayyab Chaudhry, Software Transactional Memory on GPUs.
- Rafia Inam, An A* Algorithm for Graphics Processors.
- Feng Si, Build a website to add and search events.
- Farnaz Moradi och Asrin Javaheri, Clock synchronization in sensor networks for civil security.
- Amir Bazine, Yildrim Zaynal, D.E.V.A.S - A Distributed Enterprise Vulnerability Assessment Scanner.
- Pauline Gomér, Jon-Erik Johnzon, Visualisations of network (Internet) traffic.
- Jonas Bengtsson, Growing security overlay networks.
- Stefan Berglund, Using end-point security to prevent information leakage.
- Christian O. Andersson, Study of Bluetooth propagated malware.
- Alireza Tamadoni, Process for performing a Business Impact Analysis.
- Benoit Bertholon, Integrity issues in global computing platforms.
- Jonas Åhdal: Shared Resource for Collaborative Editing over Wireless Networks.
- Karl Molin: Measurement and Analysis of the Direct Connect Peer-to-Peer File Sharing Network.
- Yang Yang and Xiaochu Wang: Forecasting short term traffic conditions using vehicular ad-hoc network.
- Ilhan Uludag: Validating reservation-base MAC algorithms for vehicular ad-hoc network.
- Ali Reza Sayar: Test and analysis of intrusion prevention using personal firewalls. Rapporten innehåller tester och utvärderingar av personliga brandväggar med avseende på säkerhet och användarvänlighet.
- Sheikh Mahbub Habib, Syed Zubair: Security Evaluation of the Windows Mobile Operating System. Arbetet ledde till flera vetenskapliga publikationer.
- Lander Casado: Security in Wireless Sensor Networks. Arbetet har resulterat i vetenskaplig publikation. I detta arbete implementerades symmetrisk kryptografiska rutiner i det sensornätverk som vi arbetar med i samarbete med Saab.
- Davide Bozza: Analysis and development of people tracking system and sensor networks. I detta arbete studerades hur data från kameror kan kombineras med sensornätverksdata (speciellt passive infraröda detektorer). Denna kombination övervinner problem som de enskilda sensorerna har, till exempel vid överlappande objekt. Arbetet gjordes från University of Torino.
- Johan Claeson: RS232 – RJ45 network adapter for an Echelon “Data Concentrator”.

Bilaga 4: Medverkan i kommittéer, paneler, konferenser, etc. för Tema 4

Forskarna inom Tema 4 är aktiva medlemmar i det internationella forskningssamhället och deltar i ett antal programkommittéer och andra vetenskapligt relevanta konstellationer. Vissa av dessa har finansierats direkt av projektet och listas nedan. Listan innehåller även exempel på andra vetenskapliga fora, som vi bedömer är av intresse för MSB och där aktörer inom forsknings-projektet har medverkat.

- Erland Jonsson är medlem i det vetenskapliga rådet för programmet Center for Networked Security, som leds av Swedish Institute of Computer Science (SICS).
- Erland Jonsson medverkade i EasyFairs paneldebatt med temat Säkerhet – tänker vi rätt, i Göteborg, 13 januari 2009.
- Erland Jonsson är ämnesredaktör på International Journal of Information Security och hanterar fortlöpande ett antal bidrag till denna tidskrift.
- Erland Jonsson, Magnus Almgren, Ulf Larson och Philippas Tsigas har genomför granskningar av ett antal bidrag till International Journal of Information Security.
- Erland Jonsson var granskare för tidskriften IEEE Transactions on Software Engineering's Special Issue on Software Dependability.
- Erland Jonsson var medlem i programkommittén för MetriSec 2010, den främsta konferensen som är inriktad mot säkerhetsmetrik.
- Erland Jonsson var medlem i programkommittén för DIMVA 2009, Sixth Conference on Detection of Intrusions and Malware & Vulnerability Assessment.
- I samband med årsredovisningen presenterade Erland Jonsson och Philippas Tsigas forskningsprojektet för MSBs ledning 29 januari 2009, med ett speciellt fokus på delprojektet med sensornätverk.
- Erland Jonsson presenterade forskningsprojektet vid Security Arena vid ett referensgruppsmöte 2 februari 2009.
- Marina Papatriantafilou med doktoranden Zhang Fu deltog i 2nd DYNAMO (Dynamic Communication Networks) Workshop, Dagstuhl, 2-6 juni 2009.
- Marina Papatriantafilou är medlem i styrgruppen för Minema och också i kommittén för Dynamo.
- Marina Papatriantafilou är medlem i programkommittén för 8th International Conference on Ad hoc Networks and Wireless (AdHocNow 2009), 22-25 september 2009, Spanien. http://libra.inf.um.es/~pedrom/adhocnow/
- Marina Papatriantafilou är medlem i programkommittén för the 13th International Conference On Principles Of DIstributed Systems (OPODIS 2009), Nimes, France, 15-18 december 2009. http://www.opodis.net/
- Marina Papatriantafilou är medlem i programkommittén för the 3rd International Conference Wireless Applications and Computing 2009, (WAC 2009): Algarve, Portugal, 17- 19 juni 2009.
- Marina Papatriantafilou är medlem i programkommittén för the 5th International Workshop on Algorithmic Aspects of Wireless Sensor Networks (Algosensors 2009), in conjunction with ICALP'09, Rhodes, Greece, 10-11 juli 2009. www.algosensors.org/algosensors09/
- Tomas Olovsson är medlem i programkommittén för NordSec 2009, the 14th Nordic Conference on Secure IT Systems, Oslo, Norge. 14-16 oktober 2009.
- Tomas Olovsson är medlem i programkommittén för CISIS'09 - Second International Workshop on Computational Intelligence for Security in Information Systems.

- Tomas Olovsson var talare på Virtualization Summit 2009 i Kista 11 februari 2009, där han presenterade Säkerhet vid virtualisering, möjligheter och hot.
- Erland Jonsson var inbjuden som gäst på en workshop organiserad av EU-projektet ThinkTrust. Workshopen avhölls i Bryssel 24-25 februari 2009.
- Tomas Olovsson kommer att deltaga i IDGs paneldebatt om IT och framtiden i Sälen den 22-23 mars.
- Vilhelm Verendel talade på Security Arena den 24 augusti 2009: Sociala nätverk och Kriskommunikation. Ämnet berörde utmaningar och metoder att designa säkra och robusta nätverk för kommunikation i kristider.
- Tomas Olovsson var talare på Aqeri Tech Summit 2009: Network security, Next generation. Presentationen handlade om hur nästa generation av nätverksskydd bör byggas där man inte bara använder brandväggar på traditionellt sätt.
- Erland Jonsson föredrog vid SRA (Society for Risk Analysis) i Karlstad, (30 juni 2009).
- Erland Jonsson föredrog på en EU-konferens med temat The Knowledge Triangle – Shaping the future of Europe i Göteborg (1 september 2009). Han berättade där om framgångarna vi haft med Security Arena och hur Triple Helix-strukturen kan vara ett verksamt sätt att åstadkomma den eftersträvade Knowledge Triangle, (1 september 2009).
- Erland Jonsson har haft ett möte med EU-organisationen Joint Research Centre (JRC – 16 september 2009) för att diskutera hur krishantering sker i Sverige och hur en europeisk samordning kan åstadkommas.
- Magnus Almgren deltog i ett möte på Lindholmen Science Park för att redovisa den akademiska forskningen för VINNOVA (28 april).
- Dennis Nilsson hade ett möte med Volvo VTEC för att diskutera telematik och säkerhet, 2009-05-07.
- Magnus Almgren deltog i konferensen RAID 23-25 september 2009 i Frankrike.
- Anna Gryszkiewicz och Fang deltog i Euro-Atlantic Stakeholder Conference (EASC) i Stockholm, 1-2 oktober 2009.
- Anna Gryszkiewicz deltog i konferensen Vad kan Sverige lära av kriser? i Stockholm den 2 september.
- Anna Gryszkiewicz deltog i ISCRAMs sommarskola i Tilburg: Citizen Participation in Crisis Response. (En av de lyckade aspekterna med denna sommarskola var att organisatörerna hade blandat doktorander av olika discipliner. Detta ledde till diskussioner av ämnen från olika perspektiv. Undervisningen sträckte sig från tekniska ämnen, med t.ex. *mashups* till mer sociala aspekter. Till exempel föredrog representanter från FN om samarbete mellan olika organisationer.)
- Fang Chen deltog på ITS-konferensen 2009 i Stockholm.
- Andreas Larsson, Anna Gryszkiewicz, Fang Chen, Vilhelm Verendel och Erland Jonsson deltog på ISCRAM 2009 (Information Systems for Crisis Response and Management), 10-13 maj 2009 i Göteborg.

Vidare medverkar Philippas Tsigas i följande konstellationer:

- MiNEMA (Middleware for Network Eccentric and Mobile Applications, European Network) Steering Committee member (2003–)
- OPODIS (International Symposium on Principles of Distributed Computing) Steering Committee member. (1998–)

- EUROPAR (European Conference on Parallel Computing) Advisory Committee member. (2000–)
- Medlem i programkommittén för the 23rd IEEE International Parallel and Distributed Processing Symposium (IPDPS 2009) Rom, Italien.
- Granskar bidrag till IEEE Transactions on Depandable and Secure Computing.
- European Science Foundation (ESF), reviewers (experts) pool, (2006-)
- Vid the Irish Research Council for Science, Engineering and Technology (IRCSET), motsvarande det svenska Vetenskapsrådet, utvärderar Philippas Tsigas ansökningar.
- Medlem i den kanadensiska motsvarigheten till det svenska Vetenskapsrådet, Natural Sciences and Engineering Research Council of Canada (NSERC). Han kommer att delta i detta råd 2007–2012.
- Medlem i programkommittén för the 29th Conference on Distributed Computing Systems (ICDCS 2009) som ägde rum juni 2009 i Montreal, Kanada.
- ICDCS 2010 – Program Chair for the Algorithms and Theory track, the Program Committee of the 30th Conference on Distributed Computing Systems. ICDCS 2010 går av stapeln i Genua, Italien.
- ICDCN 2010 – Program Committee of the 11th International Conference on Distributed Computing and Networking. ICDCN 2010 går av stapeln Kolkata, India.
- MCC 2009 – serving on the Program Committee of the 2nd Swedish Workshop on Multi-Core Computing. MCC 2009 äger rum i Uppsala, Sweden.
- Var medlem i programkommittén för the 15th International Conference On High Performance Computing (HIPC 2007) som ägde rum i december 2008 i Bangalore, Indien. Han är medlem även i nästa års programkommitté, alltså för HiPC 2009.
- High Performance Computing. HIPC 2009 äger rum i Kochi, Indien.
- PPoPP 2010 – External reviewer for the 15th ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming. 9-14 januari 2010, Bangalore, Indien.
- Distributed Computing, Journal, Elsevier.
- International Journal of Information Security, Elsevier.

Bilaga 5: Publikationer för Tema 1

I denna bilaga listas de publikationer och tekniska rapporter, som tagits fram inom ramen för projektet.

- TT släppte artikel/news release 6 december 2008 (hamnpilot)
- Sveriges Radio publicerade en nyhetsnotis 7 december 2008 (hamnpilot)
- Göteborgsposten publicerade tidningsartikel 7 december 2008 (hamnpilot)
- Västnytt gjorde ett inslag på en minut, där Bo Norrhem intervjuades 7 december 2008 (hamnpilot)
- Smålandsposten publicerade artikel på Internet 6 december 2008 (hamnpilot)
- Norrköpings Tidningar publicerade en artikel på nätet 8 december 2008 (hamnpilot)
- PåHuGGeT (logistiktidning via mail) publicerade en notis 11 december 2008 (Lindholmen Science Park: stöldfokus, med Volvo) (hamnpilot)
- Branschnyheter.se publicerade en artikel 8 december 2008 (hamnpilot)
- Transportnet.se (Transport iDag och Logistik iDAGs nättidning) publicerade en artikel tisdag 9 december 2008 (hamnpilot)
- Västsvenska Industri- och Handelskammaren publicerade en notis 10 december 2008 (hamnpilot)
- Åkeri & Transport publicerade artikel i nr 1/februari 2009 (hamnpilot)
- Tidningen Älvstranden publicerade artikel i nr 1 2009 (hamnpilot)
- Finalist (1 av 3) för pris som Årets säkerhetslösning, en del av Stora Logistik och Transportpriset – prisutdelning 27 april 2009 på Svenska Mässan (hamnpilot)
- Svenska Dagbladet 23 september (Demoteatern vid ITS kongressen)
- Dagens Industri 24september (Demoteatern vid ITS kongressen)
- Technology Magazine publicerade artikel i nr 4 20009 (nov) som gavs i samband med TechEvent Safety & Security (hamnpilot)
- Branschtidningen Proffs publicerade artikel i nr 11 2009 (nov) (hamnpilot)

LINDHOLMEN
SCIENCE PARK

LINDHOLMEN SCIENCE PARK AB
Box 8077, 402 78, Göteborg
Besöksadress: Lindholmspiren 5
Tel: 031 764 70 00
Fax: 031 764 70 50
Org nr: 556568-6366
www.lindholmen.se