Operationer i cyberdomänen

En inventering av svensk forskning

HENRIK KARLZÉN, HELENA GRANLUND OCH MIKAEL WEDLIN

FOI-R--4594--SE
ISSN 1650-1942 Maj 2018

Henrik Karlzén, Helena Granlund och Mikael Wedlin

Operationer i cyberdomänen

En inventering av svensk forskning

Bild: Henrik Karlzén/wordle.net

Titel	Operationer i cyberdomänen – en inventering av svensk forskning
Title	Operations in the cyber domain – an inventory of Swedish research
Rapportnr/Report no	FOI-R--4594--SE
Månad/Month	Maj
Utgivningsår/Year	2018
Antal sidor/Pages	175
ISSN	1650-1942
Kund/Customer	Försvarsmakten
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Cyber
Projektnr/Project no	E72737
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem
Exportkontroll	Innehållet är granskat och omfattar ingen information som är underställd exportkontrollagstiftningen.

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

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

Sammanfattning

Denna rapport beskriver en inventering av de fem senaste årens forskning om operationer i cyberdomänen som utförts av svenska organisationer. Forskningsområdet rör antagonistiska hot mot datorer i nätverk. Inventeringen baserades på en analys av de 883 forskningsartiklar som identifierades genom databassökning i Scopus. De organisationer som författat artiklarna utgörs av tre forskningsinstitut, fyra företag samt 22 universitet och högskolor. Hälften av organisationerna har författat under 25 artiklar vardera, medan resterande producerat 27–215 artiklar var. 108 artiklar utgör resultat av samarbeten mellan två till fyra av de svenska organisationerna. Vidare har en dryg tredjedel av artiklarna någon annan än en svensk organisation som huvudförfattare. Området delades in i 38 delområden och genom en jämförelse med tidigare inventeringar identifierades vissa av delområdena som nya eller växande. Här märks framförallt sakernas internet, trådlösa sensornätverk, cyberfysiska system, resursbegränsade enheter, molnet, virtualisering, positionsinformation, kultur, sociala nätverk, cybermobbning, artificiell intelligens, anomalidetektering, lägesuppfattning och nätfiske. Utöver artiklarna studerades också organisationernas egna forskningspresentationer, vilket delvis gav en annan bild. En särskild jämförelse mellan FOI:s forskning och de andra organisationernas forskning gjordes också. Tydligast är att FOI, till skillnad från de flesta andra har ett klart militärt fokus samt att FOI:s artiklar i första hand rör administrativa skydd och tekniska skydd som intrångsdetektering och lägesuppfattning, men inte kryptografi, biometri, hårdvarunära aspekter eller forensik. Slutligen föreslås att utvecklingen följs närmare genom att denna typ av inventering görs ofta samt att en liknande inventering utförs för internationell forskning.

Nyckelord: operation, cyberdomän, inventering, säkerhet, forskningsområde, nyckelord

Summary

This report describes an inventory of the last five years of Swedish research on operations in the cyber domain. The field focuses on antagonistic threats to networked computers. The inventory was mainly conducted by analysing the 883 research papers identified by searching the Scopus database with some manual filtering. Of the organisations authoring the papers there were three research institutes, four companies and 22 universities. Half of the organisations have produced less than 25 papers, whereas the remaining produced 27–215 each. 108 of the papers were authored in cooperation between two to four of the organisations. In addition, over a third of the papers' principal author is of a foreign organisation. The research area was divided into 38 sub-areas. By comparison with previous inventories, certain sub-areas were identified as new or growing. This is primarily the case of the internet of things, wireless sensor networks, cyber-physical systems, resource-limited devices, the cloud, virtualisation, position integrity, culture, social networks, cyber bullying, artificial intelligence, anomaly detection, situation awareness and phishing. In addition to the papers, the organisations' own research descriptions were also studied, which partly painted a different picture. A special comparison between FOI's research and the other organisations' research was also conducted. The most distinct differences are that FOI, unlike most organisations, has a distinct military focus, and that FOI's papers primarily concern administrative protective measures and technical solutions such as intrusion detection and situation awareness, but not cryptography, biometrics, hardware aspects or forensics. Finally, it is suggested that developments be followed closely by repeating this type of inventory and that a similar inventory is conducted for international research.

Keywords: operation, cyber, domain, review, inventory security, research, keyword

Innehållsförteckning

1 Inledning

Regeringens dokument *Nationell strategi för samhällets informations- och cybersäkerhet* (Regeringskansliet, 2017) lyfter fram att den globala digitaliseringen medför fantastiska möjligheter för samhället men också risker:

”Digitaliseringen är ett globalt fenomen och påverkar i stort sett alla delar av vårt samhälle. Det medför stora möjligheter, men också risker. Hur vi hanterar riskerna som följer av digitaliseringen har stor betydelse för vår förmåga att upprätthålla och stärka både vårt välstånd och vår säkerhet. Informations- och cybersäkerhet är idag en fråga som angår hela samhället.”

För att hantera dessa risker har bland annat Försvarsmakten en uttalad uppgift att *”stärka skyddet av Sverige i cyberrymden”* (Försvarsmakten, 2016). För att *”säkerställa tillgång till kunskap och kompetens”* samt för att *”kunna fatta strategiska beslut om långsiktig inriktning och förmågeutveckling”* (Försvarsmakten, 2018) har Försvarsmakten därför nyligen skapat det nya forskningsområdet *operationer i cyberdomänen*. I linje med detta har Försvarsmakten uppdragit åt FOI att inventera svensk forskning för att ta reda på vad det redan forskas om i Sverige och vilken kompetens som finns var. Denna inventering beskrivs i denna rapport.

Eftersom forskningsområdet är nytt och saknar tydliga gränser är inventeringen bred varför rapporten även kan vara av intresse för andra intressenter än Försvarsmakten. Rapporten kan utgöra ett underlag för de som har behov av, eller arbetar med, kunskapsutveckling inom forskningsområdet eller närliggande sådana. Rapporten erbjuder också en bred översikt av området för alla som är intresserade av vilken forskning som bedrivs inom området i Sverige.

1.1 Forskningsområdets definition och avgränsning

Forskningsområdet *operationer i cyberdomänen* är inte entydigt definierat. I avsnitt 1.1.1 beskrivs därför olika definitioner av cyberdomänen. Därefter beskriver avsnitt 1.1.2 definitioner av operationer i allmänhet samt mer specifikt operationer i cyberdomänen. Tillsammans vägleder definitionerna vilken forskning som inkluderas i den här forskningsinventeringen, vilket beskrivs närmare i avsnitt 1.1.3.

En del av definitionerna i de följande avsnitten kommer från ordböcker. Dessa definitioner är på en övergripande nivå och kan i någon mån ses som objektiva, men till kostnad av viss otydlighet.

Andra definitioner kommer istället från olika organisationer i den globala militära försvarssektorn. Dessa definitioner tar utgångspunkt i den specifika organisationens syn vilket ger specificitet, men också subjektivitet.

1.1.1 Cyberdomänen

I USA, som på många sätt är ett föregångsland inom detta område, definierades begreppet cyberrymd (vilket kan användas ekvivalent med begreppet cyberdomän) redan 2009, i en bok beställd av amerikanska försvarsdepartementet (vår översättning):

”[Cyberrymden är] en global domän inom informationsmiljön vars distinkta och unika karaktär inramas av dess användning av elektronik och det elektromagnetiska spektrumet för att skapa, lagra, modifiera, utbyta eller exploatera information via ömsesidigt beroende och sammankopplade nätverk med hjälp av informations- och kommunikationsteknik” (Kuehl, 2009)

I den svenska doktrinen nämns inte cyberdomän, men om cyberrymden sägs följande:

”Cyberrymden är den del av informationsmiljön som består av de sammanlänkade och av varandra beroende IT-infrastrukturer med tillhörande data och information. Den inkluderar internet, intranät, telekommunikationssystem, datorsystem samt inbyggda processorer och styrenheter.” (Försvarsmakten, 2016)

Formuleringen *sammanlänkade och av varandra beroende* är snarlik den amerikanska. I den svenska militärdoktrinen står det också att:

”Gränsen mellan ekonomiska, kriminella, militära och politiska aktörer flyter ihop [...] Cyberrymden innebär strategiskt ett globalt gränslöst utrymme för att på distans genomföra attacker, underrättelsetjänst, påverkan, opinionsbildning och propaganda. Försvarsmaktens resurser ska stödja defensiva och offensiva operationer i syfte att stärka skyddet av Sverige i cyberrymden.” (Försvarsmakten, 2016)

I definitionerna återkommer det att cyberdomänen

- är global och gränslös
- använder elektronik, det elektromagnetiska spektrumet och IT
- är till för att skapa, lagra, modifiera, utbyta eller exploatera information
- medger verkan på distans på grund av infrastrukturer som är sammanlänkade och av varandra beroende
- rymmer både angrepp och skydd samt underrättelser, propaganda och opinionsbildning.

1.1.2 Operationer i cyberdomänen

I Svensk ordbok (Svenska Akademien, 2009) definieras i första hand *operation* som *”Avgränsad handling med bestämt syfte och ofta innehållande flera delmoment.”*

Eftersom fackuttryck ofta kommer till svenskan från engelskan är det av intresse att också notera den engelska motsvarigheten till svenskans operation. Den mest relevanta betydelsen i Oxford Living Dictionaries (2018) definierar operation som (vår översättning) *”en organiserad aktivitet involverande ett antal personer”*.

Den nu gällande övergripande svenska militärdoktrinen, (Försvarsmakten, 2016), ger också en definition:

”Operation är en sammanfattande benämning på militära handlingar eller genomförandet av uppdrag och uppgifter som, oavsett ledningsnivå, syftar till att nå ett bestämt mål inom ett område.”

USA:s militära doktrin för cyberoperationer (Joint Chiefs of Staff, 2013) definierar cyberrymdsoperationer (snarare än operationer i cyberdomänen) som (vår översättning):

”Användningen av cyberrymdsförmågor där det primära syftet är att uppnå mål i eller genom cyberrymden.”

I definitionerna återkommer det att operationer är organiserade och avgränsade handlingar med bestämt syfte och mål. Dessa syften och mål preciseras av USA-doktrinen (uppdelat på tre typer av operationer) som att:

- *”projicera makt genom appliceringen av kraft i eller genom cyberrymden”* (offensiva cyberoperationer)
- *”bibehålla förmågan att använda cyberrymdsförmågor”* (defensiva cyberoperationer)
- *”designa, bygga, konfigurera, säkra, drifta, underhålla och upprätthålla […] system och nätverk på ett sätt som bibehåller datas tillgänglighet, riktighet, konfidentialitet samt autentisering och oavvislighet”* (informationsnätverksoperationer).

Däremot ingår inte ”*rutinmässig användning av cyberrymden [...] som exempelvis […] att skicka mejl […] och skriva dokument*”.

Samma doktrin preciserar handlingarna (förmågorna):

- *”Cyberrymdshandlingar som skapar […] degradering, avbrott eller förstörelse samt manipulering.”* (cyberrymdsangrepp)

- *”Säkrande, drift och försvar […] specifika handlingar inkluderar skydd, detektering, karaktärisering, motverkande och lindring.*” (cyberrymdsförsvar)
- *”inhämtning av underrättelser som kan behövas för framtida operationer”* (cyberrymds-ISR)
- *”Icke-underrättelsehandlingar som genomförs för att planera och förbereda följande militära operationer”* (förberedelse av omgivningen för cyberrymdsoperationer)

Efter viss tolkning framgår det därmed att operationer i cyberdomänen, enligt den amerikanska doktrinen, innebär att inom cyberdomänen utföra:

- offensiv, genom att hindra, degradera, störa, förstöra eller manipulera
- försvar, genom att detektera, karaktärisera, motverka eller lindra
- underrättelseinhämtning, relevant för offensiv och försvar

1.1.3 Avgränsning och kriterier

Från definitionerna kan det konstateras att området *operationer i cyberdomänen* är brett. Som avgränsning är det dock tydligt att området har koppling till information som behandlas i datorer. Kopplingen till datorer kan vara direkt, som i ett skydd mot skadlig kod, eller indirekt som i en riskbedömning som görs för ett datorsystem.

Vidare begränsas området av att det avser datorer som är sammankopplade i nätverk. Forskning som inte direkt relaterar till nätverk kan dock ändå vara relevant, förutsatt att den lika gärna kan tillämpas på en nätverksmiljö. Dock exkluderas forskning som i huvudsak rör fysisk säkerhet (även om det gäller datorer). Dessutom krävs en relation till säkerhet i den bemärkelsen att det finns antagonister som ligger bakom hot mot datorsystemet.

Som framgår av definitionerna har en operation också ett bestämt mål. Detta kriterium beaktas dock inte i inventeringen, eftersom forskning sällan är så specifik att den går att direkt omvandla i praktik. Istället kan forskningen visa på en uppsättning mer generella metoder och tekniker som i en anpassad och mer specifik form kan nyttjas vid en operation.

1.2 Tidigare genomgångar

Som beskrevs i rapportens första avsnitt har denna forskningsinventering den tidigare genomgången av Löfvenberg (2010) som utgångspunkt. Den tidigare genomgången baserades på intervjuer med forskningsgruppsföreträdare vid universitet, högskolor, forskningsinstitut samt företag och resulterade i en beskrivning av gruppernas forskningsområden och storlek. Inom ramen för den här studien gjordes en litteratursökning som visade att ett antal andra liknande genomgångar också genomförts:

- Post- och telestyrelsen publicerade 2002 resultatet av en genomgång av IT-säkerhetsforskning i Sverige som utfördes av FOI (Post- och telestyrelsen, 2002). Genomgången baserades på en enkät som skickades ut till företrädare för olika forskningsverksamheter för att ta reda på deras forskningsområden, finansiärer och storlek.
- Handelshögskolan vid Örebro universitet rapporterade 2011 en genomgång av forskning om informationssäkerhet (Karlsson et al., 2011). Materialet inhämtades genom internetsökning, kontakt med forskningsföreträdare samt genomgång av publicerade artiklar. Enbart forskargrupper beaktades, snarare än enstaka forskare eller privata företag.
- FOI kartlade IT-säkerhets- och informationssäkerhetsutbildningar samt doktorsavhandlingar i Sverige 2015 (Hunstad och Rodhe, 2015), vilket visar på en del av förutsättningarna för forskartillväxt i Sverige.
- En statlig utredning drog 2016 slutsatsen att ”*forskning inom cybersäkerhet bedrivs vid ett stort antal universitet och högskolor. Svenska företag har också kompetens inom detta område. Forskning kring specifikt militära aspekter av området, t.ex. doktrinutveckling som belyser ett cyberförsvar integrerat i militära operationer, är däremot mindre utvecklad*” (von Sydow et al., 2016).
- KTH och Karlstads universitet genomförde 2017 på uppdrag av FOI var sin trendspaning (Dam (red.), 2017; Fritsch et al., 2017) med relevans för informationssäkerhet som skulle besvara frågan *”Vilka nya/kommande tekniker inom ert forskningsområde tror ni kan ha potential inom försvaret […] på 10-25 års sikt.*” (Överenskommelse, 2017a; Överenskommelse, 2017b)

En slutsats som kan dras är att de tidigare genomgångarnas avgränsningar varierar, likaså metoden som använts för att samla in och analysera data. Den här rapporten har ett bredare omfång än någon av de tidigare genomgångarna. Metoden som används avser att ge en konkret bild av varje organisations forskning i första hand baserat på en oberoende källa, i form av forskningsartiklar från en akademisk databas, snarare än organisationernas egna

uttalanden. Rapporten erbjuder ingen indelning i forskargrupper eftersom sådana är mer eller mindre informella. Istället hålls resultatet på organisationsnivå. Inte heller presenteras några nyckeltal om antal anställda forskare. Dock anges antal författare. Eftersom rapportens resultat baseras på en akademisk databas är urvalet bredare än om det baseras på vilka organisationer som är kända för de som genomför inventeringen eller vilka organisationsföreträdare som svarar på en enkät eller har tid med en intervju.

2 Metod

Den huvudsakliga informationsinsamlingen beskrivs i avsnitt 2.1, den följande analysen i avsnitt 2.2, en kompletterande informationsinsamling i avsnitt 2.3 samt ytterligare syntes och analys i avsnitt 2.4.

2.1 Informationsinsamling

För att erhålla aktuell och saklig information om forskningen användes databasen Scopus[1] som är den största databasen för sammanfattningar och metadata för forskningsartiklar (Agarwal et al., 2016). Inventeringen baseras på forskningsartiklar som publicerats i antingen en akademisk tidskrift eller i samband med en akademisk konferens.

Utifrån de delområden som identifierats i de tidigare genomgångarna, kriterierna från definitionstexterna som refererats (i avsnitt 1.1.3) ovan samt generella nyckelord rörande datorer (cyber) och säkerhet, bildades en preliminär söksträng. Söktermen *militär* fanns med i söksträngen, men artiklar som berörde andra domäner togs också med. Efter en inledande sökning förfinades söksträngen för att filtrera bort irrelevanta resultat. Vidare beaktades enbart artiklar inom relevanta discipliner, vilka i Scopus angavs som datavetenskap, ingenjörsvetenskap, matematik, samhällsvetenskap, företagsekonomi, energi, beslutsteori, ekonomi, psykologi och det multidisciplinära. Vidare exkluderades artiklar som även klassificerades som hörande till medicin, biokemi, materialvetenskap och miljövetenskap. Enbart artiklar publicerade under perioden 2013-01-01 till och med 2018-03-20 samt artiklar som senast 20 mars 2018 hade accepterats för publicering 2018 till och med 2019 inkluderades. Dessutom var en förutsättning att minst en av författarna var verksam vid en svensk organisation. Mer detaljer om den slutliga söksträngens uppbyggnad återfinns i bilaga 1.

Det bör noteras att även om Scopus är en mycket omfattande databas, finns det en del tidskrifter och konferenser som den inte indexerar. Till exempel har Scopus relativt litet omfång vad gäller humaniora (Agarwal et al., 2016). Å andra sidan saknar dess främsta konkurrenter viss nödvändig funktionalitet för denna studie. Web of Science kopplar inte artikelförfattare till deras organisationer medan den svenska databasen Diva inte täcker in forskningsartiklar från alla forskningsinstitut och företag. Det finns också andra typer av forskning än den som pågår inom akademin, såsom rapporter eller mer produktnära utveckling på företag eller av enskilda entusiaster som hackare. Dessa typer av forskning ingick dock inte i inventeringen eftersom det rör sig om dokument som i begränsad mån

[1] Scopus är en betaltjänst som nås på http://www.scopus.com

är inkluderade i en central databas och som inte genomgått samma typ av granskning (peer-review) som forskningsartiklar.

2.2 Analys

Efter sökningen i Scopus gjordes också en manuell filtrering av artiklar, vilket beskrivs i avsnitt 2.2.1. Dessutom gjordes en övergripande analys av artiklarna och deras metadata (avsnitt 2.2.2) samt en delområdesindelning av den forskning artiklarna beskrev (avsnitt 2.2.3).

Artiklarna delades in per organisation där organisationerna var universitet, högskolor, forskningsinstitut och företag. Enbart organisationer med minst sju träffar inkluderades. Eftersom mängden forskningsresultat varierar mellan artiklar är antalet artiklar inte ett komplett mått på omfattningen av den forskning som utförts. I en senare del av processen gjordes därför även en analys av artikelkvaliteten (se avsnitt 2.2.2).

2.2.1 Manuell filtrering av artiklar

För att filtrera bort irrelevanta artiklar som trots allt kom med i sökresultatet, utfördes också en manuell filtrering. Den manuella filtreringen gjordes oberoende av två personer i projektgruppen. För att med tanke på det nya forskningsområdets bredd vara så inkluderande som möjligt, togs alla artiklar med som åtminstone en av personerna ville behålla.

Filtreringen baserades i första hand på nyckelord satta av artikelförfattarna, i andra hand nyckelord satta av tidskriften eller konferensen när de första nyckelorden saknades och i tredje hand artikelsammanfattningen (eng. abstract) om inga nyckelord fanns. Om även sammanfattningen saknades togs artikeln inte med alls. En lista på samtliga inkluderade artiklar återfinns i bilaga 2.

2.2.2 Övergripande analys

Artiklarna och deras metadata analyserades för att avgöra hur många artiklar organisationerna publicerat inom området under vart och ett av de inkluderade åren, vilket kan ge viss trendinformation. Vidare sammanställdes antalet författare per organisation, vilket tillsammans med antalet artiklar ger viss insikt i storleken på organisationen och hur mycket fokus som finns på att publicera forskningsartiklar. Antalet artiklar där någon från organisationen står som förstaförfattare anges också. Dessutom redovisas eventuella artikelsamarbeten organisationerna hade med varandra samt eventuella samarbeten med organisationer i andra delar av världen.

Förutom analyser av mängderna är det också intressant att analysera vilken påverkan artiklarna får. Till exempel kan en forskningsartikel vara lång och fylld

med nya resultat, medan en annan kan vara kort och snarare sammanfatta andras resultat. Med andra ord ger inte antalet artiklar hela sanningen. De flesta kvantitativa måtten av en forskningsartikels påverkan baseras på hur många andra forskningsartiklar som citerar den. För varje organisation gjordes därför en analys för att etablera dess mest citerade artiklar. Det bör dock observeras att inte heller detta är ett perfekt mått. Till exempel nämner Agarwal et al. (2016) att det förutom artikelns kvalitet finns vissa ovidkommande aspekter som spelar roll för antalet citeringar, såsom antalet referenser, publiceringsdatum, var författarna kommer ifrån, författarnas kön och ålder, författarnas akademiska titlar samt vilket språk artikeln är skriven på.

Andra aspekter som påverkar antalet citeringar rör var artikeln publicerats, det vill säga publikationen. En publikation inom ett bredare och mer långsiktigt forskningsfält gör också att chanserna till fler citeringar är större än om det rör sig om ett smalt och trendkänsligt forskningsfält (Agarwal et al., 2016). Vidare brukar en publikation som det är svårare att bli publicerad i generera fler citeringar. För att bedöma publikationerna används i denna rapport den citeringsrankningskvot som beräknas i Scopus och benämns *CiteScore rank* vilken baseras på hur många som citerar publikationens artiklar relativt hur många som citerar artiklarna i andra liknande publikationer. Dessutom redovisas huruvida publikationen är en tidskrift eller om det rör sig om ett konferensbidrag.

2.2.3 Indelning i delområden

För varje organisation sammanställdes också deras forskningsdelområden, både vilka tekniker och metoder de undersökte samt till viss del inom vilka domäner. Sammanställningen av delområden utgick främst från artiklarnas nyckelord kompletterat med en del ord från artikeltitlarna. Någon vedertagen taxonomi som kunde användas för materialet hittades inte, vilket inte heller är förvånande då materialet är mycket stort och spretigt. Enskilda konferenser eller tidskrifter kan visserligen ha sin egen taxonomi, men den är ofta otydlig, och det finns ingen metataxonomi som gäller för alla konferenser och alla tidskrifter.

För varje organisation sammanfattades de vanligaste nyckelorden (eller nyckelordsklasserna) till ett mindre antal nyckelord på svenska. Denna sammanfattning var nödvändig för att göra materialet hanterbart storleksmässigt, för att kunna göra jämförelser mellan organisationer samt för att undvika sammansatta nyckelord.

Först och främst utgår alltför generella nyckelord. Till exempel är *confidentiality loss*[2], *information security* samt *security* alla säkerhetsrelaterade men alltför övergripande. Nyckelord som är snarlika läggs samman och tas med som helhet

[2] Artiklarnas nyckelord återges i detta stycke på originalspråket engelska för att inte tappa precision i översättningen. Som fackuttryck har de i flera fall inga uppenbara svenska motsvarigheter.

om nyckelorden tillsammans förekommit tillräckligt många gånger. Exempelvis är *border gateway protocol, BGP* och *BGP monitoring* mycket lika och kan tillsammans med g*ateways, routing, rounting anomalies, routing information* samt *HTTP, communication channels, campus network*, och så vidare, placeras i det gemensamma delområdet *nätverk*. På samma sätt bildar *embedded software, embedded system, embedded systems, embedded system development, modern embedded systems* och så vidare delområdet *inbyggda system*. Kryptoprotokollet *AES* kan tillsammans med bland annat *cryptographic algorithms, differential power analysis attack, key agreement* samt *perceptual hash* samlas under rubriken *kryptografi*. Dessutom passar *anonymity, computer privacy, data mining, digital oblivion, gender, personal identity, privacy, right to be forgotten* och så vidare alla i delområdet *personlig integritet.* I vissa fall är relationerna inte särskilt uppenbara men de kan ändå skönjas, till exempel då de sammanfattningar (abstracts) som nyckelorden hör till studeras. På så sätt kunde till exempel *resource-constrained devices, energy efficiency, measured energy consumption, energy utilization* samt *cost-effective solutions* sammanfattas med *resursbegränsade enheter*. På detta sätt kan hundratals nyckelord föras samman till ett mer hanterbart och överblickbart antal delområden medan nyckelord som bara används någon enstaka gång eller ger alltför knapphändig information kan sållas bort.

Det finns vissa generella begränsningar med denna typ av delområdesindelning och här återges några sådana, inspirerat av Isenberg et al. (2017) som gjort en liknande typ av indelning (inom ett annat område):

- **Gränsdragningen mellan olika delområden är inte alltid rättfram** (Isenberg et al., 2017)
  Ett exempel på hur detta beaktats i inventeringen är att två snarlika eller nära besläktade delområden ändå hållits åtskilda på grund av att betydande mängder forskning finns på vart och ett av delområdena samt i vissa fall att olika organisationer genomgående använder olika begrepp. Att då välja det ena begreppet skulle utgöra ett ställningstagande för den ena organisationen framför den andra.

- **En del delområden kan bli mer allmänna än andra**
  Exempelvis kan indelarens kunskap eller inriktning göra att vissa nyckelord verkar snarlika medan en expert eller särskilt intresserad skulle ha gjort en tillräckligt stor åtskillnad för att de skulle behandlas som separata delområden (Isenberg et al., 2017). Detta innebär att inventeringens författare subjektivt påverkar resultatet.

- **Nyckelord saknar ibland den kontext som behövs**
  Av denna anledning kan inte nyckelorden tolkas på ett tillräckligt specifikt sätt för att de ska kunna gå att delas in i delområden (Isenberg et al., 2017). I de fall där kontexten upplevts oklar har den här inventeringen därför även nyttjat artikeltitlar och sammanfattningar för

att bringa klarhet. Det kan dock trots allt ha inträffat att artiklar associerats med fel delområden, om kontexten varit vilseledande.

2.3 Kompletterande informationsinsamling och analys

Varje organisations sammanställda delområden kompletterades med hur organisationerna, eller enskilda hos organisationerna, själva beskriver sin forskning på deras webbplatser. Det är viktigt att observera att denna bild inte nödvändigtvis stämmer överens med den som fås från forskningsartiklarna. Forskningsartiklarna visar på vad som gjorts, medan hemsidorna kan tänkas vara mer inriktade på vad som kommer att göras, eller åtminstone vad organisationerna vill göra. Denna webbplatsgenomgång är dessutom enbart av exempelkaraktär och inte ett försök att hitta all information som organisationerna vill uttrycka. Webbplatsgenomgången gjordes för alla organisationer som inkluderades från Scopus. Dessutom gjordes webbplatsgenomgången också för övriga svenska universitet och högskolor, men inget relevant hittades från dessa, vilket kan tas som en bekräftelse av Scopus-sökningens lämplighet.

2.4 Analys av delområdena som helhet

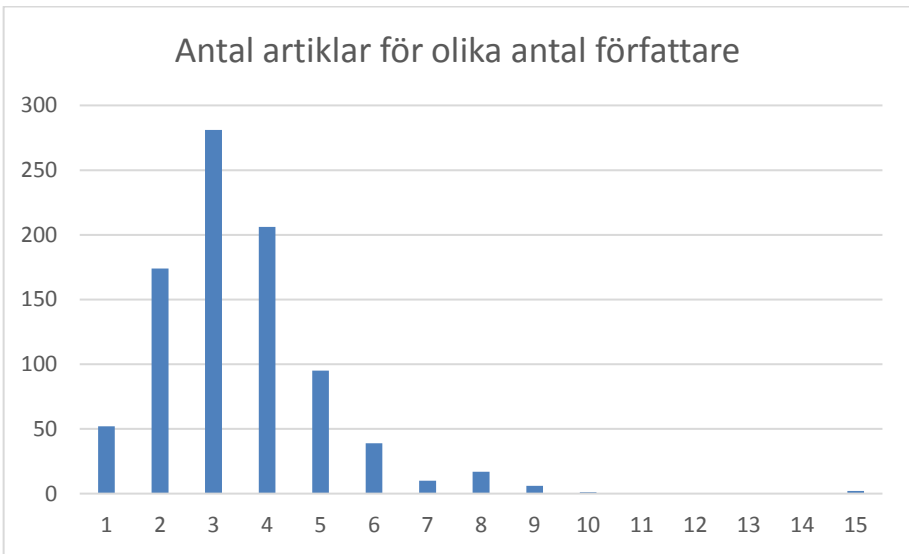
En analys genomfördes också av den svenska forskningen som helhet. En jämförelse mellan resultatet och söktermerna gjordes för att se om det var några söktermer som inte genererade något resultat. Vidare gjordes en jämförelse med tidigare genomgångar för att se trender. Därutöver identifierades vissa delområden som en enstaka organisation eller ett fåtal organisationer är ensamma om att forska om. Dessutom gjordes en analys av vilka delområden andra organisationer än FOI publicerat inom men inte FOI.

3 Resultat

Avsnitt 3.1 beskriver övergripande resultat, avsnitt 3.2 går in på varje organisations forskning medan avsnitt 3.3 beskriver forskningsområdet som helhet.

3.1 Övergripande resultat

Sökningen gav 2854 artiklar innan den manuella filtreringen. Antalet artiklar efter filtreringen sjönk till 883 artiklar, det vill säga 31 % återstod. En lista på samtliga dessa 883 artiklar återfinns i bilaga 2. Antalet författarskap för dessa artiklar var 3076, där en författare som till exempel skrivit tre artiklar ger upphov till tre författarskap. Alla författare räknas med, oavsett om de hör till de här studerade organisationerna eller ej. Antalet författare per artikel varierade mellan 1 och 15 med ett snitt på ungefär 3,5 författare. Detta illustreras av Figur 1.



Figur 1 – Antalet artiklar för varje antal författare (1–15).

De Sverigebaserade artikelförfattarna var för det slutliga urvalet fördelade på 29 organisationer och av dessa är tre forskningsinstitut[3] (FOI, SICS samt SP[4]), fyra

[3] Karolinska institutet är ett universitet och räknas därför här som det, trots namnet.
[4] SICS och SP är numera båda en del av RISE Research Institutes of Sweden Holding AB men redovisas här var för sig av historiska skäl.

företag (ABB, Ericsson, Saab samt Volvo[5]) samt 22 universitet och högskolor. Därmed uppgick antalet universitet och högskolor varifrån inga relevanta artiklar hittades till åtta, eller till 26 om begreppet utbildningsanordnare ges en vidare tolkning (Universitetskanslersämbetet, 2018). De inkluderade organisationerna listas i Tabell 1 tillsammans med en indikering om huruvida de var med i någon av de tidigare genomgångarna som beskrivs i avsnitt 1.2. I tabellen ges både organisationernas fullständiga namn samt de kortnamn som används i framförallt tabeller och figurer.

Tabell 1 – Organisationerna som bedöms relevanta för denna inventering och huruvida de var med i tidigare genomgångar. Både organisationernas fullständiga namn samt deras kortnamn ges. De fullständiga organisationsnamnen för lärosätena kommer från Högskolelag (1992:1434), övriga från respektive organisations hemsida. De tidigare genomgångarna är PTS, 2002 (Post- och telestyrelsen, 2002); FOI, 2010 (Löfvenberg, 2010); ORU, 2011 (Karlsson et. al, 2011).

Kortnamn	Organisation	Genomgång			
		PTS, 2002	FOI, 2010	ORU, 2011	Här
ABB	ABB[6]				●
Blekinge	Blekinge tekniska högskola	●	●	●	●
Borås	Högskolan i Borås				●
Chalmers	Chalmers tekniska högskola	●	●	●	●
Ericsson	Ericsson AB[7]	●	●		●
FHS	Försvarshögskolan[8]			●	●
FOI	Totalförsvarets forskningsinstitut[9]	●	●	●	●
Göteborg	Göteborgs universitet				●
Halmstad	Högskolan i Halmstad				●
Karlstad	Karlstads universitet	●	●	●	●
Karolinska	Karolinska institutet				●

[5] Både Volvo Car Corporation och Volvo Group sorterar under benämningen Volvo i denna inventering.
[6] http://new.abb.com/se
[7] https://www.ericsson.com/en
[8] https://www.fhs.se/
[9] https://foi.se/

Kortnamn	Organisation	Genomgång			
		PTS, 2002	FOI, 2010	ORU, 2011	Här
Kristianstad	Högskolan Kristianstad				●
KTH	Kungl. Tekniska högskolan	●	●	●	●
Linköping	Linköpings universitet	●	●	●	●
Linné	Linnéuniversitetet				●
Luleå	Luleå tekniska universitet	●	●	●	●
Lund	Lunds universitet		●	●	●
Malmö	Malmö universitet				●
Mitt	Mittuniversitetet				●
Mälardalen	Mälardalens högskola				●
Saab	Saab AB[10]				●
SICS	RISE SICS AB[11]	●	●	●	●
Skövde	Högskolan i Skövde		●	●	●
SP	Sveriges Tekniska Forskningsinstitut[12]				●
Stockholm	Stockholms universitet	●	●	●	●
Umeå	Umeå universitet				●
Uppsala	Uppsala universitet				●
Volvo	Volvo Car Corporation[13] samt Volvo Group[14]				●
Örebro	Örebro universitet			●	●

[10] https://saabgroup.com/sv/
[11] https://www.sics.se/about-rise-sics
[12] https://www.sp.se/sv/about/Sidor/default.aspx
[13] https://www.volvocars.com/intl
[14] http://www.volvogroup.se/sv-se/about-us/organization.html

I de följande avsnitten presenteras organisationernas nyckeltal (avsnitt 3.1.1), samarbeten mellan organisationerna (avsnitt 3.1.2), samarbeten med andra länders organisationer (avsnitt 3.1.3) samt de tidskrifter och konferensserier där artiklarna publicerats (avsnitt 3.1.4).

3.1.1 Organisationernas nyckeltal

Tabell 2 visar hur många artiklar varje organisation publicerat. Medan det finns ganska många organisationer som ligger mellan 30 och 50 artiklar, är det mycket få som väsentligen överstiger 50 (vilket motsvarar ungefär en i månaden). En observation som kan göras i anslutning till föregående avsnitt är att flera organisationer med ganska betydande publicering inte synts i tidigare genomgångar. Framförallt kan Uppsala universitet, med över 50 artiklar, noteras, men också Göteborgs universitet samt Högskolan i Halmstad har ganska betydande antal artiklar utan att ha synts tidigare. En liknande sökning för tidigare år visar inte på att dessa organisationer nyligen börjat sin forskning inom området, vilket annars hade kunnat vara en förklaring. Det bör observeras att på grund av samarbeten mellan organisationerna blir summan av varje organisations artiklar 1004 medan antalet unika artiklar är 883.

Tabellen visar också på varje organisations antal artikelförfattare, det vill säga hur många författare som skrivit minst en artikel vid organisationen. De medförfattare som inte var verksamma vid organisationen är inte medräknade, det vill säga samarbeten med andra organisationer syns inte här utan belyses istället i de kommande avsnitten. Det bör observeras att antalet författare bara delvis överlappar med antal anställda eftersom en del anställda inte publicerar sig och en del författare rör sig mellan organisationer under den relevanta tiden. Vidare visar tabellen också per organisation antalet författare dividerat med antalet artiklar. De flesta organisationer ligger kring en författare per artikel. Om en organisation till exempel har många författare som inte är så produktiva blir medelantalet författare per artikel högt. Om en organisation istället har ett fåtal och mycket produktiva författare blir det unika antalet författare per artikel snarare lågt och under ett.

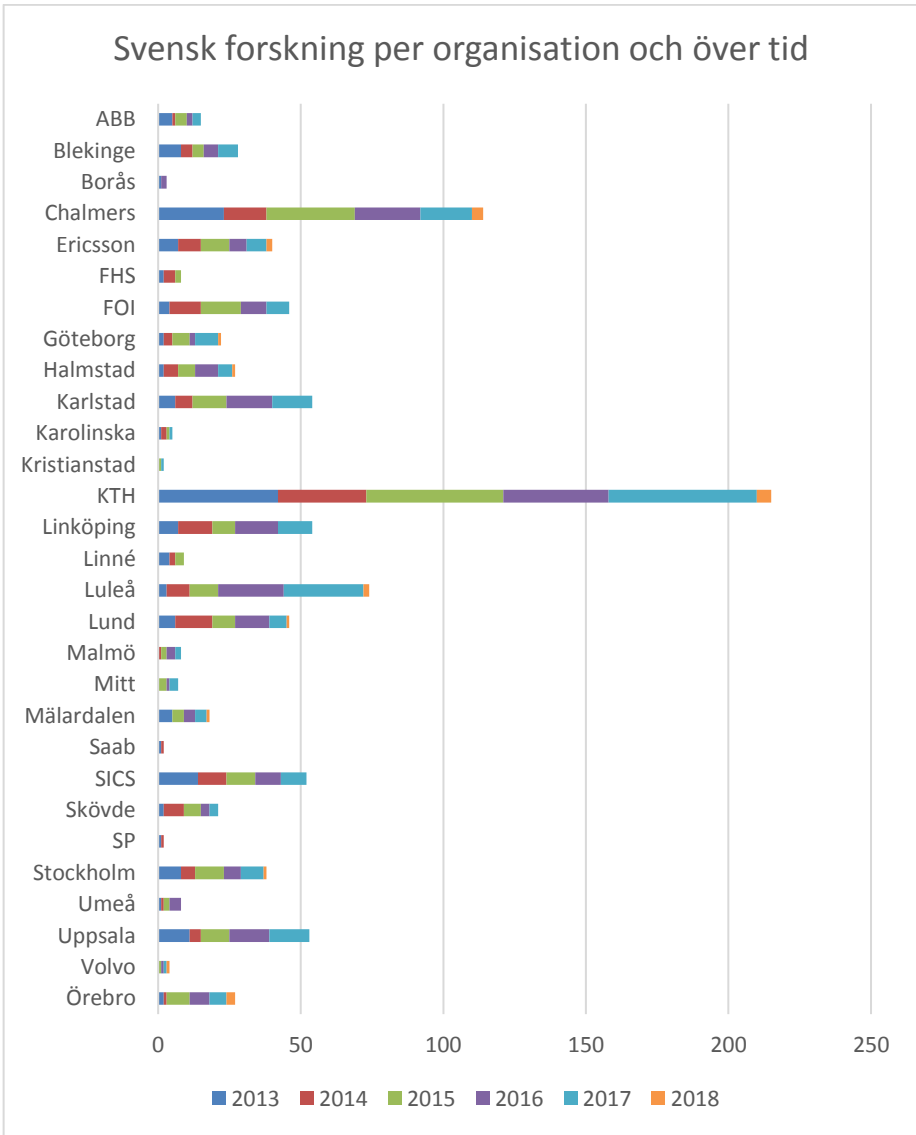
En artikel har oftast flera författare och i regel är det den som står först i listan på författare som varit mest drivande eller skrivit mest. Tabellen visar därför också hur många artiklar där någon från organisationen står som förstaförfattare och hur stor andel av organisationens artiklar detta utgör. Denna andel är 58 % i medeltal och ungefär hälften ligger på 60–90 % och den andra hälften på 30–60 % (med ett fåtal undantag).

Tabell 2 – Antal artiklar och författare per organisation samt hur många artiklar varje organisation står som förstaförfattare på.

Organisation	Artiklar	Förf.	Antal författare dividerat med antal artiklar	Förstaförf.	Procent förstaförf. av sina artiklar
ABB	15	11	0,7	13	87
Blekinge	28	32	1,1	13	46
Borås	2	3	1,5	1	50
Chalmers	115	85	0,8	71	61
Ericsson	40	43	1,1	12	30
FHS	8	7	0,9	7	88
FOI	46	44	1,0	34	74
Göteborg	22	22	1,0	8	36
Halmstad	27	21	0,8	16	59
Karlstad	54	34	0,6	27	50
Karolinska	5	9	1,8	2	40
Kristianstad	2	1	0,5	1	50
KTH	215	159	0,7	141	66
Linköping	55	42	0,8	26	47
Linné	9	7	0,8	7	78
Luleå	74	42	0,6	30	41
Lund	46	51	1,1	33	72
Malmö	8	5	0,6	7	88
Mitt	7	3	0,4	0	0
Mälardalen	18	21	1,2	9	50
Saab	2	2	1,0	1	50

Organisation	Artiklar	Förf.	Antal författare dividerat med antal artiklar	Förstaförf.	Procent förstaförf. av sina artiklar
SICS	52	24	0,5	38	73
Skövde	21	20	1,0	12	57
SP	2	5	2,5	2	100
Stockholm	39	50	1,3	25	64
Umeå	8	14	1,8	4	50
Uppsala	53	41	0,8	21	40
Volvo	4	4	1,0	1	50
Örebro	27	19	0,7	15	56
Totalt	**1004 (883 unika)**	**821**	**1,0 (medel)**	**578 (65 % av de 883)**	-

Figur 2 redogör för hur många artiklar varje organisation publicerat per år under den relevanta tidsperioden. Värdena för 2018 är låga pga. att hela året inte ingår i inventeringen samt att det finns en fördröjning mellan publicering och inkludering i Scopus.



Figur 2 – Svensk forskning per organisation och över tid (2013–2018).

3.1.2 Samarbeten mellan organisationerna

Av de 883 artiklarna är 108 artiklar samarbeten mellan organisationerna, det vill säga där artikelförfattarna kommer från flera av de svenska organisationerna. 25 av de totalt 29 organisationerna har ett samarbete med en annan av organisationerna (inom Sverige) avseende artikelförfattande (Tabell 3). De 108

artiklarna har resulterat i totalt 229 deltaganden i samarbeten, vilket bara är drygt dubbelt så många som antalet artiklar. Med andra ord är det få gånger fler än två av organisationerna samarbetar på en och samma artikel. Andelen av artiklarna som är samarbeten skiljer sig åt mellan organisationerna. Vissa har inget, eller nästan inget, samarbete alls (Högskolan i Borås, Högskolan i Halmstad, Högskolan Kristianstad, SP, Luleå tekniska universitet). Mest anmärkningsvärt är Luleå tekniska universitet som bara har ett samarbete med de andra organisationerna trots hela 74 författade artiklar som helhet. Kanske spelar det geografiska läget roll. Även Umeå universitet samarbetar i låg utsträckning. Detsamma gäller dock inte Mittuniversitetet som hör hemma i Östersund och Sundsvall, vilket också är på ett relativt stort geografiskt avstånd från potentiella samarbetspartner. Vissa organisationer har å andra sidan en samarbetsandel som tyder på att alla deras artiklar skett i samarbete med de andra organisationerna. Bland dessa märks Mittuniversitetet, Saab och Volvo.

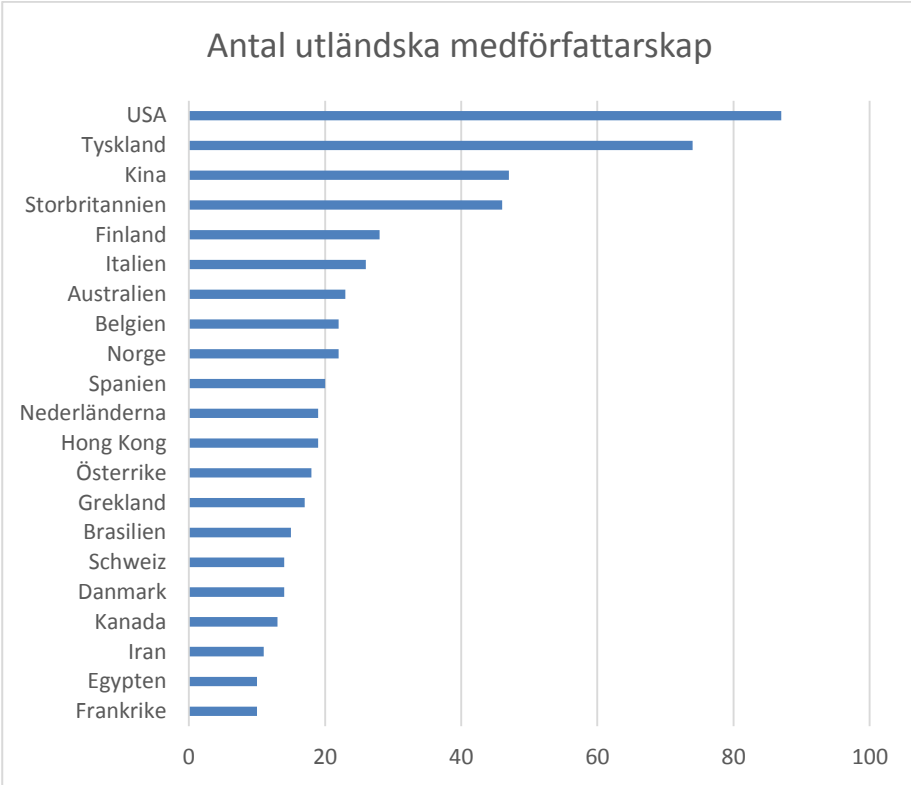
Tabell 3 – Antal artiklar per organisation med samarbete inom Sverige samt andelen av det totala antalet artiklar som är ett resultat av samarbeten.

Organisation	Antal artiklar med samarbeten	Procent artiklar med samarbeten
ABB	7	47
Blekinge	4	14
Borås	0	0
Chalmers	17	15
Ericsson	23	58
FHS	1	13
FOI	15	33
Göteborg	8	36
Halmstad	0	0
Karlstad	3	6
Karolinska	1	20
Kristianstad	0	0
KTH	37	17
Linköping	7	13

Organisation	Antal artiklar med samarbeten	Procent artiklar med samarbeten
Linné	2	22
Luleå	1	1
Lund	9	20
Malmö	3	38
Mitt	7	100
Mälardalen	10	56
Saab	2	100
SICS	25	48
Skövde	7	33
SP	0	0
Stockholm	8	21
Umeå	1	13
Uppsala	21	40
Volvo	4	100
Örebro	6	22
Medel	**8**	**30**

3.1.3 Samarbeten med andra länder

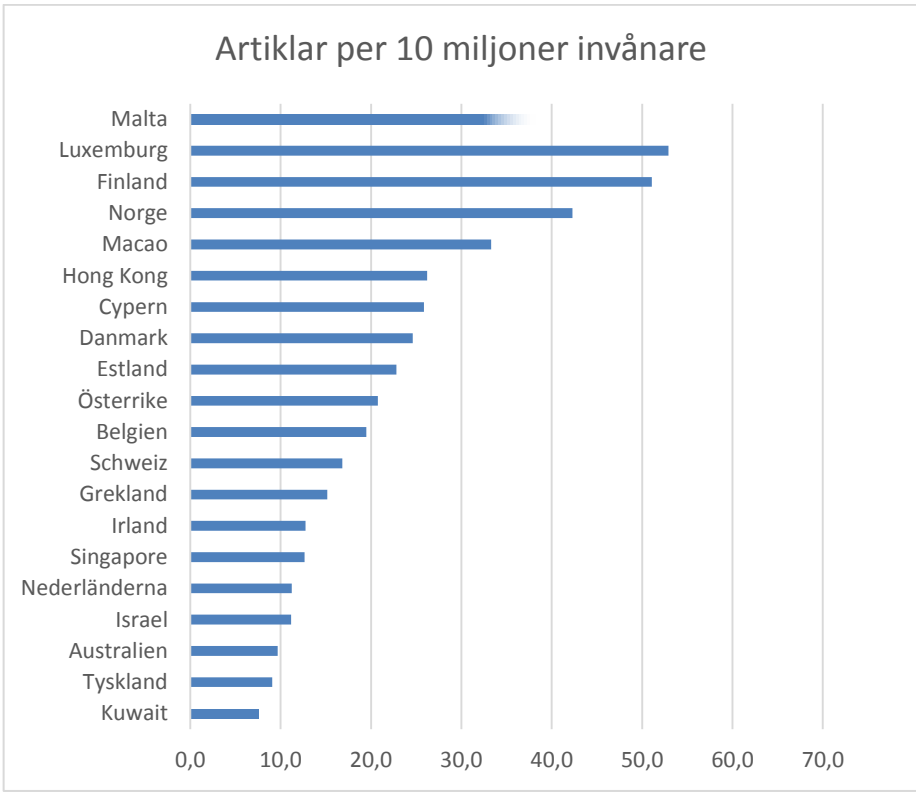
Förutom samarbeten mellan organisationerna (inom Sverige) finns en hel del samarbeten med författare som är verksamma utomlands. Figur 3 ger det totala antalet samarbeten för de länder som har minst tio samarbeten. För en artikel kan en svensk organisation samarbeta med noll, en eller flera utländska organisationer, varför figuren inte nödvändigtvis visar antal artiklar, utan antalet medförfattarskap, från varje land. Om en utländsk författare från ett visst land är med på två artiklar räknas det alltså som två medförfattarskap för det landet. Totalt uppgick de utländska medförfattarskapen till 690, vilket utgör 22 % av alla författarskapen. Om dessa författarskap vore jämnt fördelade över artiklarna skulle nästan varje artikel (av de 883) ha en utländsk medförfattare. På 35 % av artiklarna stod en utländsk författare som förstaförfattare (i enlighet med vad som beskrevs i Tabell 2).



Figur 3 – Antal utländska medförfattarskap indelat per verksamhetsland.

De länder med flest antal medförfattarskap per capita presenteras i Figur 4. Länder med mycket små populationer har flest (Malta, Luxemburg, Macao[15], Cypern, Estland) tillsammans med de nordiska länderna (Finland, Norge, Danmark) samt Hong Kong[16] och Österrike. Ungefär hälften av varje figurs länder förekommer i båda figurerna, det vill säga ungefär hälften av de länder som ligger i topp per capita är också det även när ingen hänsyn tas till befolkningsmängd.

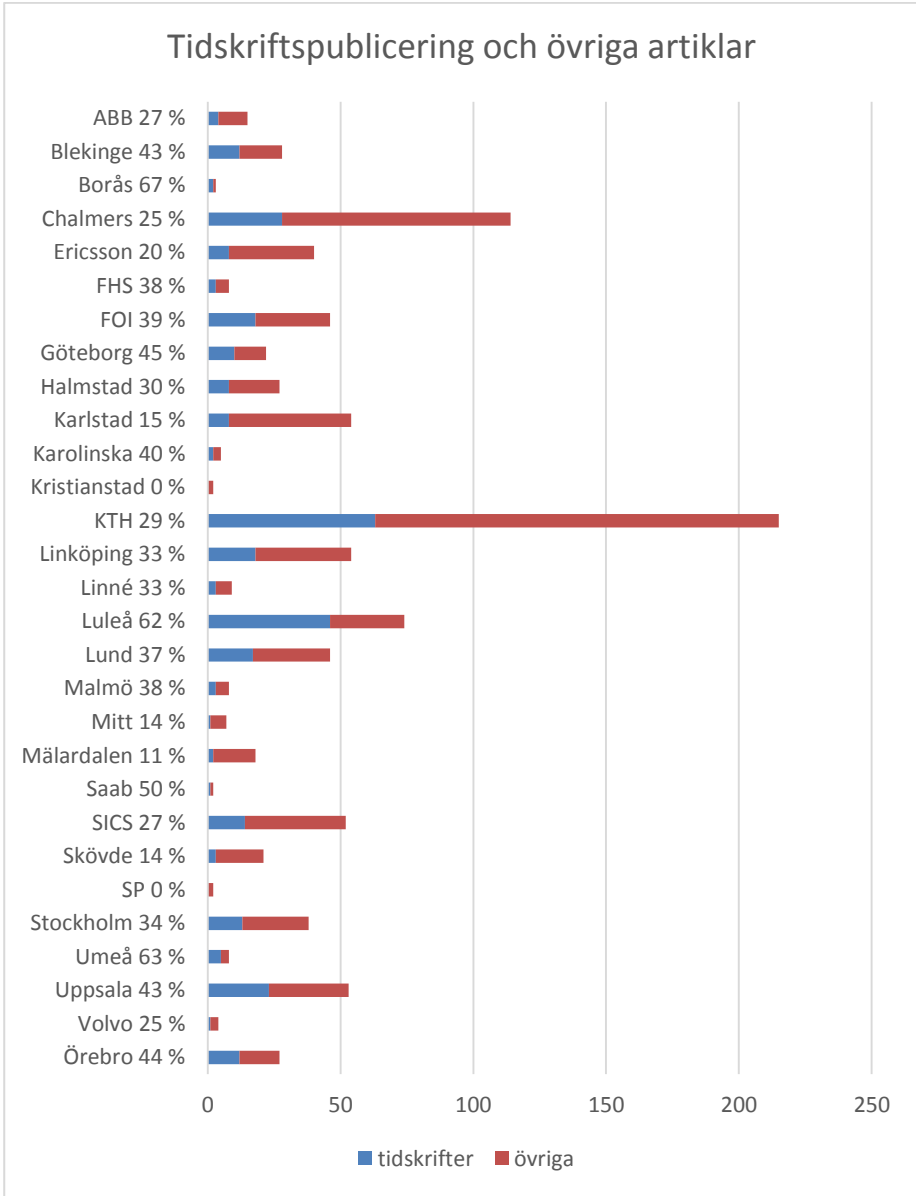
[15] Speciell administrativ region i Kina
[16] Speciell administrativ region i Kina



Figur 4 – Topp 20 länder för antal medförfattarskap per 10 miljoner invånare (Malta = 164). Populationsstorlek från (Förenta Nationerna, 2017).

3.1.4 Publikationer

Figur 5 anger hur stor andel av artiklarna som publicerats i tidskrifter respektive övriga fora (främst konferenser), indelat per organisation. Det är få organisationer som har mer än femtio procent tidskriftspublicering. Mest utmärkande bland de med fler än ett fåtal artiklar är Luleå tekniska högskola som har hela 62 % tidskriftspublicering. Något samband mellan antal artiklar eller författare och tidskriftspubliceringstendensen verkar inte finnas.



Figur 5 – Hur många artiklar varje organisation publicerat i tidskrifter respektive övriga artiklar (främst konferensbidrag).

Tabell 4 redogör för de 18 viktigaste publikationerna (källorna, att skilja från artiklarna som är de forskningsalster som tillsammans samlas i publikationer) i bemärkelsen var flest av artiklarna publicerats. De 18 publikationerna står för en

tredjedel av alla artiklar. Totalt finns hela 435 olika publikationer representerade för de 883 artiklarna, det vill säga varje publikation används ungefär två gånger i medeltal. Det bör observeras att flera av publikationerna är av en generell typ som kan liknas vid förlag som till exempel å en konferens vägnar ger ut en publikation med konferensbidragen som en del av en större serie. Dessa indikeras med ett S (för serie) i kolumnen Typ. Övriga är antingen tidskrifter (T) eller konferenspublikationer (K). Dessutom visas varje publikations citeringsrankningskvot (kolumnen CRK) vad gäller antal citeringar jämfört med andra publikationer som av Scopus klassificeras som inom samma område. Citeringsrankningskvoten, som beräknats av Scopus, är lägre (bättre) när publikationen har fler citeringar inom sitt område eftersom publikationens ranking då är närmare första plats (täljaren är lägre). I de fall en publikation ligger inom flera områden ges här ett medelvärde för dess citeringsrankningskvoter. I tre fall utelämnas kvoten eftersom den saknas i Scopus. Länkar till publikationerna återfinns bland referenserna i avsnitt 5.2.

Tabell 4 – Var organisationerna främst publicerar sig. Publikationsnamnen har förkortats för att rymmas på en rad. Nyckel: typ av publikation (Typ: S = serie; T = tidskrift; K = konferens); citeringsrankningskvot (CRK); antal artiklar (#); % av alla artiklar (%).

Publikation	**Typ**	**CRK**	**#**	**%**
L Notes in Computer Science/AI/Bioinformatics	S	0,7	119	13
IFIP Advances in Information and Comm Tech	S	0,8	25	3
ACM Intl Conference Proceeding Series	S	0,9	17	2
Computers and Security	T	0,0	15	2
Communications in Computer and Info Science	S	0,8	13	1
Information and Computer Security	T	0,5	10	1
ACM Conference on Computer and Comm Security	K	0,1	10	1
L Notes Institute Comp Sci, Soc-Informatics & Telecom	S	0,9	9	1
Annual Hawaii International Conf on System Sci	K	-	9	1
Security and Communication Networks	T	0,4	9	1
Procedia Computer Science	S	0,4	9	1
Intl Symp on Human Aspects of Info Sec & Assurance	K	-	9	1
IFAC-PapersOnLine	S	0,8	7	1
Future Generation Computer Systems	T	0,0	7	1

Publikation	Typ	CRK	#	%
IEEE Transactions on Dependable and Secure Comp	T	0,1	7	1
European Intelligence and Security Informatics Conf	K	-	7	1
Computers in Human Behavior	T	0,1	7	1
Advances in Intelligent Systems and Computing	S	0,8	6	1
Övriga (417 stycken)	**-**	**-**	**590**	**67**

3.2 Organisationerna

I det kommande avsnitten beskrivs organisationerna var för sig, däribland FOI (som denna rapports författare tillhör).

Varje organisations avsnitt inleds med en lista på organisationens forskningsdelområden, vilka utvunnits ur deras forskningsartiklar.

Efter listan på delområden kommer i förekommande fall forskningsbeskrivningar baserade på organisationernas webbplatser, följt av en tabell som kortfattat beskriver deras mest citerade artiklar. Därefter kommer en tabell över var de främst publicerar sig.

Slutligen följer, i förekommande fall, en figur som visar organisationens artikelsamarbeten med andra organisationer. Finns ingen figur för en organisation innebär det att organisationen inte haft några artikelsamarbeten med de andra organisationerna.

3.2.1 ABB

Organisationens forskning är inriktad på trådlösa sensornätverk, molnet, sakernas internet, åtkomstkontroll, tillit, mobiler, industri[17], hälsa och kryptografi.

Forskningen för en av organisationens flitigaste författare beskrivs som ”*trådlösa protokoll och förbättring av säkerheten i industriell automatisering*”, vilket stämmer väl med den artikelbaserade beskrivningen ovan (ABB, 2018).

De mest citerade artiklarna som återges i Tabell 5 berör framförallt sakernas internet och hälsa samt tillit vilket också väl överensstämmer med nyckelorden.

[17] Med *industri* avses i denna rapport det snävare begreppet (i Svensk ordbok (Svenska Akademien, 2009) definierat som *näringsgren som bygger på till-verkning och förädling i större skala vanligen med maskiner)* och inkluderar därmed inte hela det privata näringslivet.

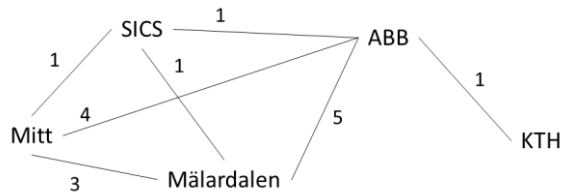
Tabell 5 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Pang Z., et al., 2015)	44	Interoperabilitet, säker mjukvaruleverans och skyddade patientdata hos hälsotjänster (sakernas internet) hemma hos folk, speciellt den allt äldre populationen.
(Kang K., et al., 2014)	25	Sakernas internet-tjänsters beteende utvärderas gentemot användarnas förväntningar på tillit.
(Pang Z., et al., 2013a)	20	Öppen och monopolundvikande plattform för hälsotjänster (sakernas internet) hemma hos folk.

Var organisationen främst publicerar sig beskrivs i Tabell 6 medan organisationens samarbeten med andra svenska organisationer ges av Figur 6. ABB har alltså samarbetat på en artikel med SICS, fyra med Mittuniversitetet, fem med Mälardalens högskola och en med KTH. En del av dessa samarbeten har skett på en och samma artikel, vilket också syns genom pilarna och siffrorna mellan de övriga organisationerna (exempelvis tre samarbeten mellan Mittuniversitetet och Mälardalens högskola) för de totalt sju artiklarna.

Tabell 6 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
IECON Proceedings (Industrial Electronics Conference)	2	13
IEEE Transactions on Industrial Informatics	2	13
Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST	1	7



Figur 6 – Organisationens samarbeten, med sju artiklar.

3.2.2 Blekinge tekniska högskola

Organisationen forskar med inriktning på personlig integritet, sakernas internet, molnet, mjukvara, skadlig kod, kryptografi, diverse angrepp, tillit, forensik och risk.

Som belysande exempel på aktuella projekt finns på organisationens hemsida beskrivet ett projekt om sakernas internet där artificiell intelligens ska nyttjas för ökad säkerhet (BTH, 2018a) samt ett projekt om att mäta säkerhetsmognaden hos mjukvaruutvecklare (BTH, 2018b).

Vidare handlar de mest citerade artiklarna om smarta hem respektive riskanalyser (Tabell 7).

Tabell 7 – Organisationens mest citerade artiklar.

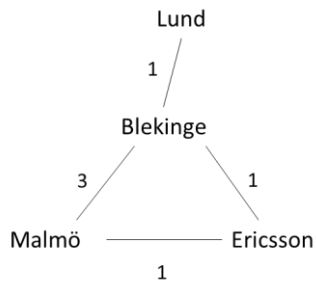
Artikel	Cit.	Sammanfattning
(Jacobsson A., et al., 2016)[18]	38	Gängse säkerhetsfunktioner ger god säkerhet i smarta hem, undantaget risker pga. humanfaktorer.
(Baca D., et al., 2013)	14	Motåtgärdsgrafer är kostnadseffektiva för riskanalyser i agil mjukvaruutveckling.

Var organisationen främst publicerar sig beskrivs i Tabell 8 medan organisationens samarbeten med andra svenska organisationer ges av Figur 7.

[18] Samma artikel är också bland de mest citerade för Malmö universitet.

Tabell 8 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	4	14
Proceedings of IEEE East-West Design and Test Symposium, EWDTS	3	11
Digital Investigation	2	7



Figur 7 – Organisationens samarbeten, med fyra artiklar.

3.2.3 Högskolan i Borås

Organisationen forskar om kryptografi, personlig integritet och molnet.

Som belysande exempel på organisationens hemsida finns en forskare vars intressen inkluderar kommunikativ interaktion i tjänstemöten, teknologi i tjänster och negativa kundbeteenden (HB, 2018).

Den mest citerade artikeln berör personlig integritet och molnet (Tabell 9).

Tabell 9 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Lindh M., et al., 2016)	3	Analys av en policy för en internettjänst visar att det görs svårt för användarna att förstå vad deras personliga data används till.

Var organisationen främst publicerar sig beskrivs i Tabell 10. Artikelsamarbeten med de andra organisationerna har inte förekommit.

Tabell 10 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Uncertainty Modelling in Knowledge Engineering and Decision Making - Proceedings of the International FLINS Conference, FLINS	1	33
European Educational Research Journal	1	33
Journal of Business Communication	1	33

3.2.4 Chalmers tekniska högskola

Forskningen fokuserar enligt artiklarnas nyckelord på trådlösa sensornätverk, mjukvara, kryptografi, biometri, överbelastningsangrepp, safety[19], mobiler, nätverk, fordon, personlig integritet, åtkomstkontroll, positionsinformation[20], tillit och artificiell intelligens.

Enligt organisations hemsida forskas det om bland annat språkbaserad säkerhet (mjukvara) och positionsinformation (CTH, 2018a), vilket stämmer väl överens med nyckelorden. Mindre tydlig är kopplingen till nyckelorden vad gäller den forsknings som på webbplatsen beskrivs röra autonoma, inbyggda och

[19] Engelskans s*afety* indikerar den typ av faror som inte uppkommer till följda av antagonister. Delområdet *safety* har dock i rapporten alltid koppling till antagonistiska hot (*security).* Till exempel hamnar där forskning som rör en domän som i stor utsträckning präglas av *safety* men med visst inslag av *security.*

[20] På engelska används begreppet *position integrity* men eftersom *integrity* både kan översättas integritet (som i personlig integritet) och riktighet, används här istället positionsinformation.

distribuerade enheter samt sakernas internet (CTH, 2018b). Nyckelordet trådlösa sensornätverk och domänen uppkopplade fordon har dock anknytning hit. Åtminstone en del forskare säger sig mer specifikt forska om de närliggande delområdena cyberfysiska system och resursbegränsade enheter (CTH, 2018c). Forskningen om kryptografi kan tydliggöras genom att nämna en forskare som enligt (CTH, 2018c) undersöker blockkedjor samt en annan forskare som enligt (CTH, 2018d) forskar om ett antal aspekter inom teoretisk kryptografi.

Tabell 11 redovisar de mest citerade artiklarna. Dessa artiklar ger specifika exempel på forskningen om tillit, mjukvara, fordon och personlig integritet.

Tabell 11 – Organisationens mest citerade artiklar.

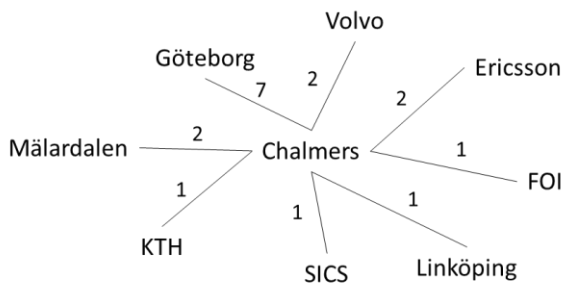
Artikel	Cit.	Sammanfattning
(Ghazawneh A., et al., 2013)	104	Egenskaper för lyckad tredje-partsutveckling föreslås, inklusive rörande tillitsaspekten.
(Hedin D., et al., 2014)	52	En del webbplatser är mindre restriktiva med användares känsliga information i informationsflöden än andra.
(Hendrickx J., et al., 2015)	26	Sårbarhetsanalys rörande falskdataangrepp på ett industriellt mätsystem visar sig vara ett problem som inte verkar ha en effektiv (polynomisk) lösning.
(Ebadi H., et al., 2015)[21]	19	Information kan utvinnas ur en mängd individdata utan att den personliga integriteten hos en enda enskild individ påverkas alltför mycket.
(Broberg N., et al., 2013)	19	Vanliga programmeringsspråk saknas utförliga möjligheter att kontrollera informationsflöden. Därför föreslås ett programmeringsspråk baserat på Java med stöd för statisk kontroll av en informationsflödespolicy.

[21] Samma artikel är också bland de mest citerade för Göteborgs universitet.

Var organisationen främst publicerar sig beskrivs i Tabell 12 medan organisationens samarbeten med andra svenska organisationer ges av Figur 8.

Tabell 12 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	30	26
IFIP Advances in Information and Communication Technology	4	4
ACM International Conference Proceeding Series	4	4



Figur 8 – Organisationens samarbeten, med 17 artiklar.

3.2.5 Ericsson AB

Forskningsartiklarnas främsta nyckelorden är åtkomstkontroll, molnet, mobiler, kryptografi, skadlig kod, sakernas internet och resursbegränsade enheter. Dessutom framkommer det av flera artikeltitlar att artiklarna också rör virtualisering.

På hemsidan finns exempel på forskning om lättviktig säkerhet för sakernas internet (Ericsson, 2018a), regelefterlevnad och molnet (Ericsson, 2018b).

De mest citerade artiklarna handlar om mobiler, kryptografi, sakernas internet och överhuvudtaget resursbegränsade enheter (Tabell 13).

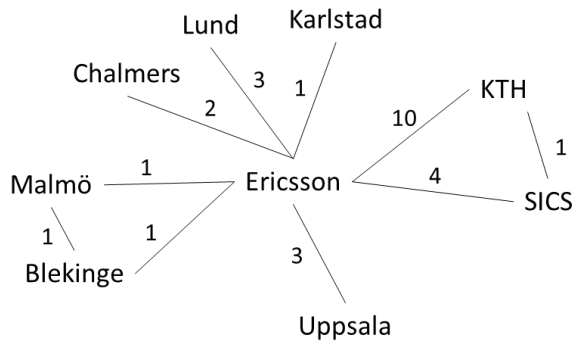
Tabell 13 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Da Silva J., et al., 2014)	29	För att öka täckning och energieffektiviteten hos säkra mobilnät kan kommunikation som går från enhet till enhet utnyttjas.
(Simplicio Jr., et al., 2013)	14	Lättviktiga krypton för trådlösa sensornätverk föreslås.
(Raza S., et al., 2016)	11	Infrastrukturer för publika kryptoinfrastrukturer (PKI:er) är alltför tungrodda för sakernas internet, men å andra sidan är alternativet med förhandsdelade nycklar inte skalbart.

Var organisationen främst publicerar sig beskrivs i Tabell 14 medan organisationens samarbeten med andra svenska organisationer ges av Figur 9.

Tabell 14 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	8	20
Proceedings - IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom	2	5
IEEE Conference on Communications and NetworkSecurity, CNS	1	3



Figur 9 – Organisationens samarbeten, med 23 artiklar.

3.2.6 Försvarshögskolan (FHS)

Forskningen berör risk och militär domän.

De mest citerade artiklarna handlar om terrorism och hotinformationsdelning (Tabell 15).

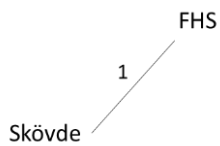
Tabell 15 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Heickerö R., 2014)	4	Al-Qaedas agerande i cyberdomänen studeras.
(Sigholm J., et al., 2013)	4	Ett ramverk för offensivt kontraspionage inom cyber föreslås baserat på bland annat omfattande hotinformationsdelning.

Var organisationen främst publicerar sig beskrivs i Tabell 16 medan organisationens samarbeten med andra svenska organisationer ges av Figur 10.

Tabell 16 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
European Conference on Information Warfare and Security, ECCWS	2	25
Proceedings - European Intelligence and Security Informatics Conference, EISIC	1	13
Proceedings - IEEE Military Communications Conference MILCOM	1	13



Figur 10 – Organisationens samarbeten, med en artikel.

3.2.7 Totalförsvarets forskningsinstitut (FOI)

Forskningen handlar om diverse angrepp, anomalidetektering, intrångsdetektering, regelefterlevnad, risk, lägesuppfattning, sociala nätverk, kultur, träning och med inriktning på den militära domänen.

Webbplatsen tar upp sådant som risk (FOI, 2018a), träning (FOI, 2018a; FOI, 2018b) militärpolitiska frågor och doktrin (FOI, 2018c), semantiska tekniker för beslutsstöd samt lägesuppfattning, (FOI, 2018d) – vilket väl matchar nyckelorden – men också forensik, mjukvara, kryptologi, inbyggda system (FOI, 2018e), assurans samt industriella informations- och styrsystem (FOI, 2018a).

De mest citerade artiklarna berör lägesuppfattning, regelefterlevnad samt anomalidetektering (Tabell 17).

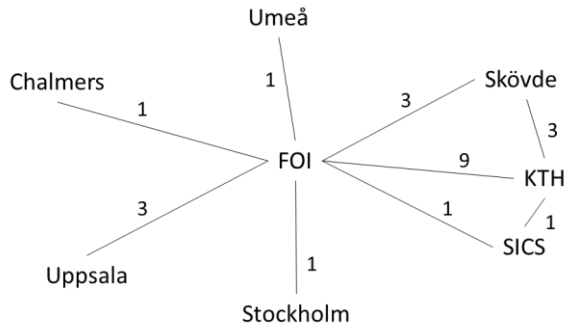
Tabell 17 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Franke U., et al., 2014)	47	En första genomgång av artiklar om lägesuppfattning inom cyber presenteras.
(Sommestad T., et al., 2014)	36	Olika variabler är olika bra på att prediktera regelefterlevnad och vilka variabler som är bäst varierar.
(Cohen K., et al., 2014)	20	Verktyg och tekniker för att detektera ensamma terrorister baserat på lingvistiska markörer studeras.
(Sommestad T., et al., 2015a)	11	Kunskap om förväntad ånger och hotuppfattning ökar prediktionsförmågan för regelefterlevnad inom informationssäkerhet mer än i gängse modell.

Var organisationen främst publicerar sig beskrivs i Tabell 18 medan organisationens samarbeten med andra svenska organisationer ges av Figur 11.

Tabell 18 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Information and Computer Security	6	13
IFIP Advances in Information and Communication Technology	2	4
Computers and Security	2	4



Figur 11 – Organisationens samarbeten, med 15 artiklar.

3.2.8 Göteborgs universitet

Forskningen fokuserar på personlig integritet, cybermobbning, sociala nätverk, safety och mjukvara.

Enligt organisationens hemsida sker också forskning om cyberfysiska system (GU, 2018).

De mest citerade artiklarna handlar om cybermobbning, personlig integritet och mjukvara (Tabell 19).

Tabell 19 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Slonje R., et al., 2013)	177	Cybermobbning som begrepp och fenomen reds ut, exempelvis med skillnaderna mot traditionell mobbning och möjlig prevention.
(Ebadi H., et al., 2015)[22]	19	Information kan utvinnas ur en mängd individdata utan att den personliga integriteten hos en enda enskild individ påverkas alltför mycket.
(Antinyan V., et al., 2014)	15	Risker inom agil mjukvaru-utveckling kan uppskattas genom komplexiteten och revisionerna av källkoden.

[22] Samma artikel är också bland de mest citerade för Chalmers tekniska högskola.

Var organisationen främst publicerar sig beskrivs i Tabell 20 medan organisationens samarbeten med andra svenska organisationer ges av Figur 12.

Tabell 20 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	3	14
IFIP Advances in Information and Communication Technology	2	9
Computers in Human Behavior	2	9

Figur 12 – Organisationens samarbeten, med åtta artiklar.

3.2.9 Högskolan i Halmstad

Forskningen fokuserar på biometri och personlig integritet.

De mest citerade artiklarna handlar om sakernas internet (något förvånande jämfört med nyckelorden ovan) och biometri, se Tabell 21.

Tabell 21 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Le A., et al., 2013)	28	Försvar mot angrepp på routing för sakernas internet bör beakta att vissa noder routar mer trafik än andra.
(Hofbauer H., et al., 2014)	26	En metod för att utvärdera det inledande steget i biometrisk iris-igenkänning föreslås för en mer finmaskig metod än att utgå från huruvida irisen känns igen.
(Mikaelyan A., et al., 2015)	8	En typ av biometrisk igenkänning baserat på området runt ögat föreslås.

Var organisationen främst publicerar sig beskrivs i Tabell 22. Artikelsamarbeten med de andra organisationerna har inte förekommit.

Tabell 22 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI)	3	11
Proceedings - International Conference on Signal-Image Technology and Internet-Based Systems, SITIS	2	7
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	1	4

3.2.10 Karlstads universitet

Forskningen fokuserar på personlig integritet, nätverk, åtkomstkontroll, molnet, intrångsdetektering, kryptografi, diverse angrepp, elektronisk röstning och tillit.

På hemsidan finns ett fokus på personlig integritet och nätverkssäkerhet beskrivet (KAU, 2018).

De mest citerade artiklarna (Tabell 23) rör cybermobbning (vilket artiklarna som helhet inte indikerade som ett återkommande delområde), personlig integritet, kryptografi och en artikel om transparent användning av personlig data i molnet.

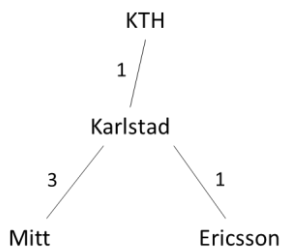
Tabell 23 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Beckman L., et al., 2013)	30	Flickor är mer involverade i cybermobbning än pojkar, jämfört med traditionell mobbning.
(Pulls T., et al., 2013)	16	Skydd mot att länka användares åtkomster över distribuerade processer för att värna den personliga integriteten.
(Winter P., et al., 2013)	14	Ett sätt att dölja data för att undvika filtrering eller censurering föreslås som baseras på morfning och en hemlighet som delas i en annan kanal.
(Fischer-Hübner S., et al., 2014)	9	Designprinciper som möjliggör transparens vid användning av andras personliga data i molnet föreslås.

Var organisationen främst publicerar sig beskrivs i Tabell 24 medan organisationens samarbeten med andra svenska organisationer ges av Figur 13.

Tabell 24 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	12	22
IFIP Advances in Information and Communication Technology	9	17
Communications in Computer and Information Science	3	6



Figur 13 – Organisationens samarbeten, med tre artiklar.

3.2.11 Karolinska institutet

Forskningen fokuserar på biometri och personlig integritet.

Den mest citerade artikeln i Tabell 25 stämmer väl med nyckelorden och lyfter fram (biobanker i) molnet som en relevant domän.

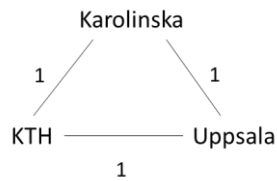
Tabell 25 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Gholami A., et al., 2014)	6	Beskriver hur EU-krav rörande personlig integritet påverkar biobanker i molnet.

Var organisationen främst publicerar sig beskrivs i Tabell 26 medan organisationens samarbeten med andra svenska organisationer ges av Figur 14.

Tabell 26 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	2	40
Procedia Computer Science	1	20
Nordicom Review	1	20



Figur 14 – Organisationens samarbeten, med en artikel.

3.2.12 Högskolan Kristianstad

Forskningen fokuserar på kryptografi.

En artikel rör identitetsbaserad kryptografi (Tabell 27).

Tabell 27 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Huang X., et al., 2015)	1	Flera aspekter hos en persons identitet läggs samman för att bilda en personlig kryptonyckel på ett säkert sätt.

Var organisationen främst publicerar sig beskrivs i Tabell 28. Artikelsamarbeten med de andra organisationerna har inte förekommit.

Tabell 28 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Proceedings - IEEE International Conference on Computer and Information Technology, CIT , IEEE International Conference on Ubiquitous Computing and Communications, IUCC , IEEE International Conference on Dependable, Autonomic	1	50
IEEE International Conference on Communications Workshops, ICC Workshops	1	50

3.2.13 KTH

Forskningen fokuserar på personlig integritet, molnet, kryptografi, nätverk, anomalidetektering, åtkomstkontroll, sakernas internet, trådlösa sensornätverk, mobiler, artificiell intelligens, nätfiske, skadlig kod, mjukvara, diverse angrepp, risk, safety, sociala nätverk, positionsinformation, cyberfysiska system, resursbegränsade enheter, fordon och virtualisering.

Hemsidan beskriver forskning om bland annat cyberfysiska system, sakernas internet, personlig integritet (KTH, 2018a) nätverk och åtkomstkontroll (KTH, 2018b)

De mest citerade artiklarna (Tabell 29) handlar om diverse angrepp, risk, positionsinformation och cyberfysiska system.

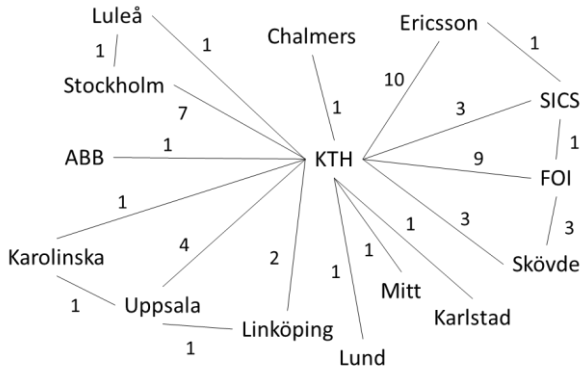
Tabell 29 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Teixeira A., et al., 2015)	95	Ett ramverk för modellering av cyberhotaktörers kunskap, resurser och intention tas fram.
(Shokri R., et al., 2014)	51	Om olika telefoner cachar och delar lägesspecifik information exponeras deras lägesuppgifter mindre till en central server än om alla frågar den direkt.
(Sommestad T., et al., 2013)	49	Ett modelleringsspråk föreslås som kan bedöma angrepps sannolikhet att lyckas lika väl som en experts bedömning.
(Sou K., et al., 2013)	45	Smarta elnäts sårbarhet mot falskdataangrepp analyseras.
(Sandberg H., et al., 2015)	41	En introduktion till cyberfysiska systems säkerhet.

Var organisationen främst publicerar sig beskrivs i Tabell 30 medan organisationens samarbeten med andra svenska organisationer ges av Figur 15.

Tabell 30 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	20	9
Computers and Security	5	2
IFAC-PapersOnLine	5	2



Figur 15 – Organisationens samarbeten, med 37 artiklar.

3.2.14 Linköpings universitet

Forskningen fokuserar enligt artiklarnas nyckelord på personlig integritet, diverse angrepp, nätverk, molnet, inbyggda system, resursbegränsade enheter, sakernas internet, åtkomstkontroll samt kryptografi.

Hemsidan beskriver forskning om åtkomstkontroll, tillit (LIU, 2018a) och kvantkryptografi (LIU, 2018b) – vilket passar med nyckelorden – men också forensik, användbarhet, intrångsdetektering, bioinformatik samt regelefterlevnad (LIU, 2018c).

De mest citerade artiklarna handlar om personlig integritet och sakernas internet, (mer specifikt smarta städer) (Tabell 31).

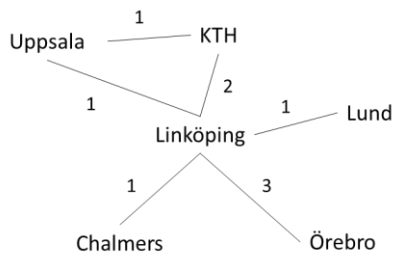
Tabell 31 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Christin D., et al., 2013)	35	Genom pseudonymer kan användares bidrag bedömas utan att användaren kan spåras mellan situationer.
(Pöhls H., et al., 2014)	24	En utgångspunkt för forskning om säkerhet, personlig integritet och tillit för sakernas internet.
(Tragos E., et al., 2014)	15	Reliabilitet och säkerhet i applikationer i smarta städer.

Var organisationen främst publicerar sig beskrivs i Tabell 32 medan organisationens samarbeten med andra svenska organisationer ges av Figur 16.

Tabell 32 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	7	13
IFIP Advances in Information and Communication Technology	2	4
ACM International Conference Proceeding Series	2	4



Figur 16 – Organisationens samarbeten, med sju artiklar.

3.2.15 Linnéuniversitetet

Forskningen fokuserar på utbildning, kryptografi, risk samt regelefterlevnad.

Hemsidan visar på forskning även om formella metoder och självskyddande system (LNU, 2018).

De mest citerade artiklarna handlar om ungas påverkan av och kunskap om, internet samt regelefterlevnad (Tabell 33).

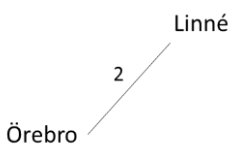
Tabell 33 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Priebe G., et al., 2013)	8	Unga reagerar olika på oönskad exponering på internet.
(Kajtazi M., et al., 2013)	3	Kunskap och resurser påverkar regelefterlevnaden.

Var organisationen främst publicerar sig beskrivs i Tabell 34 medan organisationens samarbeten med andra svenska organisationer ges av Figur 17.

Tabell 34 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Proceedings of the Australasian Conference on Information Systems	2	22
Proceedings of the Annual Hawaii International Conference on System Sciences	1	11
Proceedings of the International Symposium on Human Aspects of Information Security and Assurance, HAISA	1	11



Figur 17 – Organisationens samarbeten, med två artiklar.

3.2.16 Luleå tekniska universitet

Forskningen handlar om kryptografi, sakernas internet, personlig integritet, risk, åtkomstkontroll, biometri, molnet, överbelastningsangrepp, hälsa, mobiler, nätverk, utbildning och intrångsdetektering.

Hemsidan nämner forskning om distribuering (LTU, 2018a), nätverk, risk, infrastruktur, beteende och pedagogik – som relativt väl matchar nyckelorden ovan (LTU, 2018b).

De mest citerade artiklarna berör molnet och kryptografi (Tabell 35).

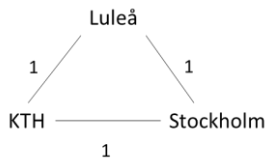
Tabell 35 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Derhamy H., et al., 2015)	30	Ramverk och plattformar för sakernas internet utvärderas baserat på kriterier som säkerhet och interoperabilitet.
(Shu Z., et al., 2016)	24	Hot mot och motåtgärder anpassade för mjukvarudefinierade nätverk presenteras.
(Yu Y., et al., 2016)	22	För att undvika komplex nyckelhantering i molnet föreslås en kryptometod som baseras på användarens identitet.
(Mohd B., et al., 2015)	18	En genomgång av statusen hos forskningen om lättviktiga blockchiffer.

Var organisationen främst publicerar sig beskrivs i Tabell 36 medan organisationens samarbeten med andra svenska organisationer ges av Figur 18.

Tabell 36 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Proceedings of the Annual Hawaii International Conference on System Sciences	5	7
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	3	4
Communications in Computer and Information Science	3	4



Figur 18 – Organisationens samarbeten, med en artikel.

3.2.17 Lunds universitet

Forskningen handlar om kryptografi, risk, personlig integritet, safety och mjukvara.

Hemsidan visar mycket riktigt på forskning om exempelvis risk (LU, 2018a) och kryptografi, men också trådlöst, sakernas internet, distribuering och fordonsnät (LU, 2018b), vilket inte matchar de artiklar som hittats i denna genomgång.

De mest citerade artiklarna berör kryptografi, personlig integritet i molnet och sexuell exponering online (Tabell 37).

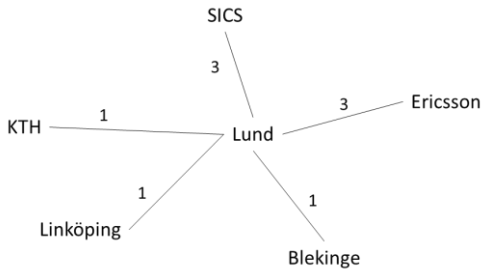
Tabell 37 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Guo Q., et al., 2014)	15	En effektivare algoritm för att knäcka krypton när bara ett antal klartext- och kryptotextpar är kända presenteras.
(Paladi N., et al., 2014)	13	En arkitektur för att öka användares kontroll av den geografiska spridningen av data I molnet.
(Jonsson L., et al., 2014)	12	Kopplingar mellan frivillig sexuell exponering online och aspekter som social bakgrund och psykosocial hälsa presenteras.
(Guo Q., et al., 2016)	10	Ett effektivt angrepp av en kryptoalgoritm presenteras.

Var organisationen främst publicerar sig beskrivs i Tabell 38 medan organisationens samarbeten med andra svenska organisationer ges av Figur 19.

Tabell 38 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	11	24
IEEE International Symposium on Information Theory - Proceedings	3	7
ACM International Conference Proceeding Series	2	4



Figur 19 – Organisationens samarbeten, med nio artiklar.

3.2.18 Malmö universitet

Forskningen fokuserar på personlig integritet, risk, sakernas internet och cybermobbning.

De mest citerade artiklarna handlar om sakernas internet (mer specifikt smarta hem), risk och personlig integritet (Tabell 39).

Tabell 39 – Organisationens mest citerade artiklar.

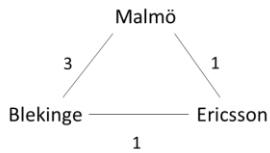
Artikel	Cit.	Sammanfattning
(Jacobsson A., et al., 2016)[23]	38	Gängse säkerhetsfunktioner ger god säkerhet i smarta hem, undantaget risker pga. humanfaktorer.
(Jacobsson A., et al., 2015)	7	Ett förslag till generell modell för personlig integritet och säkerhet I smarta hem presenteras.

Var organisationen främst publicerar sig beskrivs i Tabell 40 medan organisationens samarbeten med andra svenska organisationer ges av Figur 20.

[23] Samma artikel är också bland de mest citerade för Blekinge tekniska högskola.

Tabell 40 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Future Generation Computer Systems	1	13
Computers in Human Behavior	1	13
Proceedings - International Conference on Availability, Reliability and Security, ARES	1	13



Figur 20 – Organisationens samarbeten, med tre artiklar.

3.2.19 Mittuniversitetet

Forskningen fokuserar på kryptografi, industri och tillit.

De mest citerade artiklarna matchar väl nyckelorden och handlar om industriella tillämpningar och kryptografi (Tabell 41).

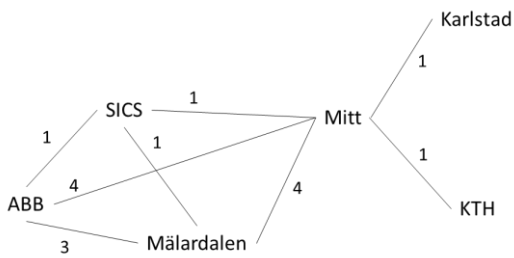
Tabell 41 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Ray A., et al., 2015)	2	Säkerhet, kapacitet och punktlighet relateras i ett industriellt nät.
(Ray A., et al., 2016)	1	Forskningsutmaningar rörande industriell kommunikationssäkerhet presenteras, såsom nyckelhantering samt relationen mellan användbarhet och säkerhet.

Var organisationen främst publicerar sig beskrivs i Tabell 42 medan organisationens samarbeten med andra svenska organisationer ges av Figur 21.

Tabell 42 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	1	14
Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST	1	14
Proceedings - International Computer Software and Applications Conference	1	14



Figur 21 – Organisationens samarbeten, med sju artiklar.

3.2.20 Mälardalens högskola

Forskningen handlar om trådlösa sensornätverk, mjukvara, industri, nätverk och safety.

Artikeltitlarna visade på att artiklarna också handlar om assurans.

Hemsidan ger exempel på trådlösa nät i industriella tillämpningar, såsom reliabel trådlös kommunikation i hårda miljöer (MDH, 2018).

De mest citerade artiklarna berör mjukvara respektive industriella trådlösa sensornät (Tabell 43).

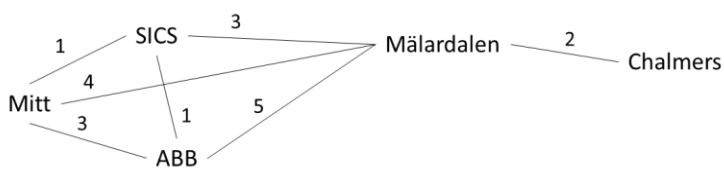
Tabell 43 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Hedin D., et al., 2015)	14	Kombinationen statisk och dynamisk informationsflödeskontroll presenteras för att hantera tilliten mellan använder och tredje part.
(Pang Z., et al., 2013b)	11	Industriella trådlösa sensornät ställer bland annat säkerhetskrav krav på realtidsoperativsystemen.

Var organisationen främst publicerar sig beskrivs i Tabell 44 medan organisationens samarbeten med andra svenska organisationer ges av Figur 22.

Tabell 44 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Proceedings of the IEEE International Conference on Industrial Technology	3	17
Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST	2	11
Proceedings - IEEE International Conference on Software Testing, Verification and Validation Workshops, ICSTW	2	11



Figur 22 – Organisationens samarbeten, med tio artiklar.

3.2.21 Saab AB

Forskningen handlar om anomalidetektering samt personlig integritet.

Den mest citerade artikeln berör anomalidetektering (Tabell 45).

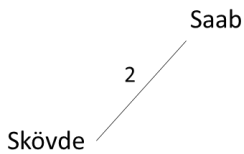
Tabell 45 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Laxhammar R., et al., 2014)[24]	24	En algoritm för anomalidetektering vid övervakning av rörliga objekt presenteras.

Var organisationen främst publicerar sig beskrivs i Tabell 46 medan organisationens samarbeten med andra svenska organisationer ges av Figur 23.

Tabell 46 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Proceedings - European Intelligence and Security Informatics Conference, EISIC	1	50
IEEE Transactions on Pattern Analysis and Machine Intelligence	1	50



Figur 23 – Organisationens samarbeten, med två artiklar.

3.2.22 SICS

Forskningen handlar om trådlösa sensornätverk, sakernas internet, kryptografi, molnet, åtkomstkontroll, resursbegränsade enheter, sakernas internet, virtualisering och nätverk.

[24] Samma artikel är också bland de mest citerade för Högskolan i Skövde.

Hemsidan bekräftar nyckelord som molnet, sakernas internet och kryptografi (SICS, 2018a), med tillägget personlig integritet (SICS, 2018a; SICS, 2018b).

De mest citerade artiklarna berör resursbegränsade enheter, nätverkskommunikation, intrångsdetektering, sakernas internet och kryptografi (Tabell 47).

Tabell 47 – Organisationens mest citerade artiklar.

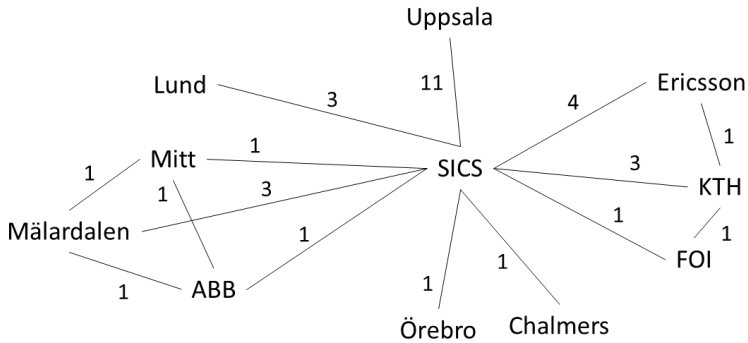
Artikel	Cit.	Sammanfattning
(Raza S., et al., 2013a)[25]	115	Lättviktig säker datagramtransport presenteras.
(Raza S., et al., 2013b)[26]	97	En lättviktig intrångsdetektering för sakernas internet presenteras.
(Wallgren L., et al., 2013)[27]	60	Angrepp mot routing för sakernas internet presenternas.
(Hummen R., et al., 2013)	41	Certifikat är trots allt ett bra sätt för autentisering i många situationer för sakernas internet.

Var organisationen främst publicerar sig beskrivs i Tabell 48 medan organisationens samarbeten med andra svenska organisationer ges av Figur 24.

Tabell 48 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	10	19
Annual IEEE International Conference on Sensing, Communication, and Networking, SECON	3	6
Computers and Security	2	4

[25] Samma artikel är också bland de mest citerade för Uppsala universitet.
[26] Samma artikel är också bland de mest citerade för Uppsala universitet.
[27] Samma artikel är också bland de mest citerade för Uppsala universitet.



Figur 24 – Organisationens samarbeten, med 25 artiklar.

3.2.23 Högskolan i Skövde

Forskningen handlar om personlig integritet, lägesuppfattning, nätfiske, anomalidetektering, mjukvara och kultur.

Hemsidan har ett exempel på ett forskningsprojekt om informationssäkerhet i kommuner (HS, 2018).

De mest citerade artiklarna rör anomalidetektering, nätfiske och lägesuppfattning (Tabell 49).

Tabell 49 – Organisationens mest citerade artiklar.

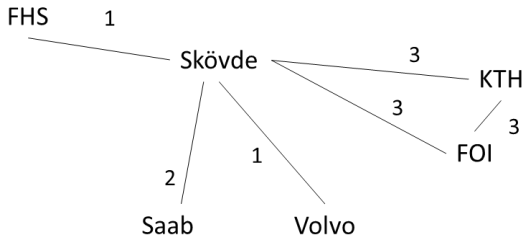
Artikel	Cit.	Sammanfattning
(Laxhammar R., et al., 2014)[28]	24	En algoritm för anomalidetektering vid övervakning av rörliga objekt presenteras.
(Flores W., et al., 2015)	7	Motståndskraften mot nätfiske beror bland annat på informationssäkerhets-medvetenhet och datorvana.
(Steinhauer H., et al., 2013)	3	Att identifiera ovisshet vid körtid möjliggör lägesuppfattning och om användaren informeras kan denne bidra med sin erfarenhet.

Var organisationen främst publicerar sig beskrivs i Tabell 50 medan organisationens samarbeten med andra svenska organisationer ges av Figur 25.

Tabell 50 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	5	24
IFIP Advances in Information and Communication Technology	2	10
International Conference on Cyber Warfare and Security , ICCWS	2	10

[28] Samma artikel är också bland de mest citerade för Saab.



Figur 25 – Organisationens samarbeten, med sju artiklar.

3.2.24 Sveriges Tekniska Forskningsinstitut (SP)

Forskningen handlar om safety och nätverk.

Hemsidan skriver om forskning om optik, tidhållning (SP, 2018a) och certifiering (SP, 2018b).

Den mest citerade artikeln berör safety och mjukvara (Tabell 51).

Tabell 51 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Soderberg A., et al., 2013)	12	Safety-kontrakt med säkerhetsimplikationer föreslås för mjukvaruutveckling.

Var organisationen främst publicerar sig beskrivs i Tabell 52. Artikelsamarbeten med de andra organisationerna har inte förekommit.

Tabell 52 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Proceedings of the Annual Precise Time and Time Interval Systems and Applications Meeting, PTTI	1	50
IEEE International Symposium on Software Reliability Engineering Workshops, ISSREW	1	50

3.2.25 Stockholms universitet

Forskningen handlar om biometri, mobiler, personlig integritet, forensik, risk, nätverk, kryptografi, utbildning och sakernas internet.

Hemsidan beskriver, i likhet med nyckelorden, forskning om informationssäkerhet, sakernas internet, risk, personlig integritet samt forensik, men också beteende, molnet och mjukvara (SU, 2018).

De mest citerade artiklarna berör beteende och risk, kryptografi och trådlösa sensornät samt kryptografi (Tabell 53).

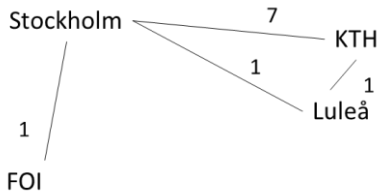
Tabell 53 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Wang Y., et al., 2016)	16	Beteende rörande sociala medier påverkas av tillit och risk.
(Toghian M., et al., 2015)	11	En metod för att distribuera krypteringsnycklar i trådlösa sensornät föreslås.
(Nawareg M., et al., 2015)	9	Ett framsteg inom kvantmekaniken som kan användas inom kryptografi presenteras.

Var organisationen främst publicerar sig beskrivs i Tabell 54 medan organisationens samarbeten med andra svenska organisationer ges av Figur 26.

Tabell 54 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Procedia Computer Science	6	16
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	4	11
IFIP Advances in Information and Communication Technology	2	5



Figur 26 – Organisationens samarbeten, med åtta artiklar.

3.2.26 Umeå universitet

Forskningen handlar om biometri, kryptografi, virtualisering och molnet.

Titlarna visade på att forskningen även handlade om diverse angrepp.

De mest citerade artiklarna berör bedömning av diverse angrepp och kryptografi (Tabell 55).

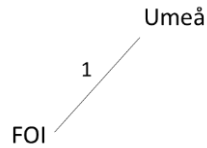
Tabell 55 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Sommestad T., et al., 2015b)	6	Ett verktyg för att prediktera angreppskonsekvenser visade sig inte kunna göra detta.
(Cao Z., et al., 2014)	4	En icke-krävande metod för att skydda sig mot avlyssning presenteras.

Var organisationen främst publicerar sig beskrivs i Tabell 56 medan organisationens samarbeten med andra svenska organisationer ges av Figur 27.

Tabell 56 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Information and Computer Security	1	13
Procedia Computer Science	1	13
Expert Systems with Applications	1	13



Figur 27 – Organisationens samarbete, med en artikel.

3.2.27 Uppsala universitet

Forskningen handlar om trådlösa sensornätverk, molnet, åtkomstkontroll, kryptografi, sakernas internet, diverse angrepp, resursbegränsade enheter, personlig integritet och artificiell intelligens.

Hemsidan bekräftar nyckelord som sakernas internet, resursbegränsade enheter, artificiell intelligens och kryptografi, men nämner också skadlig kod, informationspåverkan, formell mjukvaruutveckling och positionsinformation (UU, 2018).

De mest citerade artiklarna berör resursbegränsade enheter, intrångsdetektering, sakernas internet och åtkomstkontroll (Tabell 57).

Tabell 57 – Organisationens mest citerade artiklar.

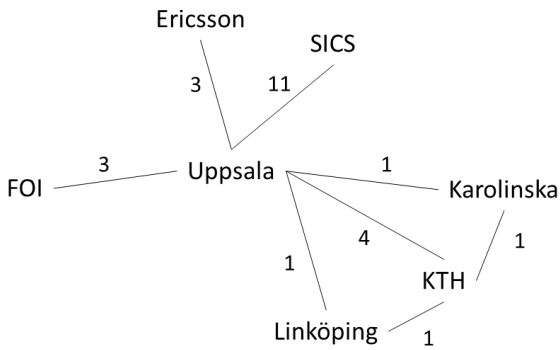
Artikel	Cit.	Sammanfattning
(Raza S., et al., 2013a)[29]	115	Lättviktig säker datagramtransport presenteras.
(Raza S., et al., 2013b)[30]	97	En lättviktig intrångsdetektering för sakernas internet presenteras.
(Wallgren L., et al., 2013)[31]	60	Angrepp mot routing för sakernas internet presenternas.
(Hummen R., et al., 2014)	34	En dedikerad server kan underlätta åtkomstkontroll och säker kommunikation i sakernas internet.

Var organisationen främst publicerar sig beskrivs i Tabell 58 medan organisationens samarbeten med andra svenska organisationer ges av Figur 28.

[29] Samma artikel är också bland de mest citerade för SICS.
[30] Samma artikel är också bland de mest citerade för SICS.
[31] Samma artikel är också bland de mest citerade för SICS.

Tabell 58 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Security and Communication Networks	2	4
IEEE International Conference on Cybercrime and Computer Forensic, ICCCF	2	4
Metrology and Measurement Systems	2	4



Figur 28 – Organisationens samarbeten, med 21 artiklar.

3.2.28 Volvo Car Corporation och Volvo Group

Forskningen handlar om fordon, risk och anomalidetektering.

Den mest citerade artikeln berör risk och fordon (Tabell 59).

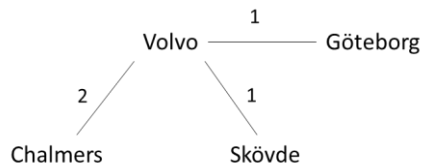
Tabell 59 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Islam M., et al., 2016)	4	Ett ramverk för riskbedömning (inklusive för antagonistisk säkerhet) för inbyggda system i bilar presenteras.

Var organisationen främst publicerar sig beskrivs i Tabell 60 medan organisationens samarbeten med andra svenska organisationer ges av Figur 29.

Tabell 60 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	1	25
IEEE Vehicular Networking Conference, VNC	1	25
CPSS - Proceedings of the ACM International Workshop on Cyber-Physical System Security, Co-located with Asia CCS	1	25



Figur 29 – Organisationens samarbeten, med fyra artiklar.

3.2.29 Örebro universitet

Forskningen handlar om hälsa, åtkomstkontroll, cybermobbning, överbelastningsangrepp, resursbegränsade enheter, sakernas internet, diverse angrepp, mobiler, regelefterlevnad, skadlig kod, nätverk och kultur.

Hemsidan nämner regelefterlevnad vilket stämmer bra med nyckelorden (ORU, 2018a), men också ett forskningsprojekt om de lite perifera moln, risk och upphandling, som dock nyligen inletts (ORU, 2018b).

De mest citerade artiklarna berör regelefterlevnad och diverse angrepp (Tabell 61).

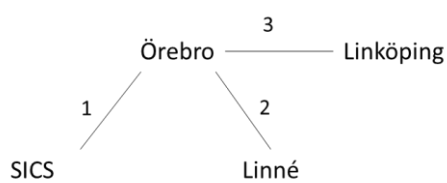
Tabell 61 – Organisationens mest citerade artiklar.

Artikel	Cit.	Sammanfattning
(Kolkowska E., et al., 2013)	22	Att förstå sambanden vid framtagandet av informationssäkerhetsbestämmelser är kritiskt för ökad regelefterlevnad.
(Conti M., et al., 2016)	21	Mannen-i-mitten-angrepp klassificeras baserat på bland annat angriparens plats i nätet och vald imitationsteknik.
(Hedström K., et al., 2013)	6	Motåtgärder bör baseras på förståelse av användares anledningar till regelbrott.

Var organisationen främst publicerar sig beskrivs i Tabell 62 medan organisationens samarbeten med andra svenska organisationer ges av Figur 30.

Tabell 62 – Var organisationen främst publicerar sig (publikation), antal artiklar i publikationen (artiklar) samt hur många procent av organisationens artiklar det utgör (% artiklar).

Publikation	Artiklar	% artiklar
Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	5	19
Information and Computer Security	3	11
IFIP Advances in Information and Communication Technology	2	7



Figur 30 – Organisationens samarbeten, med sex artiklar.

3.3 Forskningens delområden

Avsnitt 3.3.1 presenterar delområdena som helhet, avsnitt 3.3.2 undersöker eventuella uteblivna resultat från söktermerna, avsnitt 3.3.3 visar på trender gentemot tidigare genomgångar, avsnitt 3.3.4 lyfter fram ovanlig forskning och avsnitt 3.3.5 belyser vilka delområden FOI inte forskar om.

3.3.1 Delområdena som helhet

De 883 artiklarna hade 6545 nyckelord, varav 3725 var unika (i strikt mening där minsta skillnad i strängen räknas som unik). Detta resulterade i 38 delområden, indelade i sex kategorier. Kategorierna utgörs av administrativa skydd, tekniska skydd, angrepp, nätverksnära aspekter, hårdvarunära aspekter samt domän för tillämpning. Delområdena, kategorierna och vilka organisationer som forskar om vilket delområde visas i Tabell 63.

Tabell 63 – Forskningsområdets 38 delområden, kategoriserade i: administrativa skydd; angrepp; domäner för tillämpning; hårdvarunära aspekter; nätverk samt tekniska skydd. Dessutom visas vilka organisationer som publicerat artiklar inom delområdena samt hur många de är (#).

Delområde	Kategori	Forskande organisationer	#
Kultur	Admin. skydd	FOI Skövde Örebro	3
Regelefterlevnad	Admin. skydd	FOI Linné Örebro	3
Risk	Admin. skydd	Blekinge FHS FOI KTH Linné Luleå Lund Malmö Stockholm Volvo	10
Tillit	Admin. skydd	ABB Blekinge Chalmers Karlstad Mitt	5
Träning	Admin. skydd	FOI	1
Utbildning	Admin. skydd	Linné Stockholm	2
Diverse angrepp	Angrepp	Blekinge FOI Karlstad KTH Linköping Uppsala Örebro	7

Delområde	Kategori	Forskande organisationer	#
Cybermobbning	Angrepp	GU Malmö Örebro	3
Nätfiske	Angrepp	KTH Skövde	2
Skadlig Kod	Angrepp	Blekinge Ericsson KTH Örebro	4
Överbelastningsangrepp	Angrepp	Chalmers Luleå Örebro	3
Elektronisk röstning	Domän	Karlstad	1
Fordon	Domän	Chalmers KTH Volvo	3
Hälsa	Domän	ABB Luleå Örebro	3
Industri	Domän	ABB Mitt Mälardalen	3
Militär	Domän	FHS FOI	2
Personlig integritet	Domän	Blekinge Chalmers GU Halmstad Karlstad Karolinska KTH Linköping Luleå Lund Malmö Saab Skövde Stockholm Uppsala	15
Safety	Domän	Chalmers GU KTH Linköping Lund Mälardalen SP	7
Cyberfysiska system	Hårdvaru-nära	KTH	1
Inbyggda system	Hårdvaru-nära	Linköping	1
Mobiler	Hårdvaru-nära	ABB Chalmers Ericsson KTH Luleå Stockholm Örebro	7
Resursbegränsade enheter	Hårdvaru-nära	Ericsson KTH Linköping SICS Uppsala Örebro	6

Delområde	Kategori	Forskande organisationer	#
Sakernas internet	Hårdvaru-nära	ABB Blekinge Ericsson KTH Linköping Luleå Malmö SICS Stockholm Uppsala Örebro	11
Trådlösa sensornätverk	Hårdvaru-nära	ABB Chalmers KTH Mälardalen SICS Uppsala	6
Virtualisering	Hårdvaru-nära	Ericsson KTH SICS Umeå	4
Molnet	Nätverk	ABB Blekinge Borås Ericsson Karlstad KTH Linköping Luleå SICS Umeå Uppsala	11
Nätverk	Nätverk	Chalmers Karlstad KTH Linköping Luleå Mälardalen SICS SP Stockholm Örebro	10
Positionsinformation	Nätverk	Chalmers KTH	2
Sociala nätverk	Nätverk	FOI GU KTH	3
Anomalidetektering	Tekniska skydd	FOI KTH Saab Skövde Volvo	5
Artificiell intelligens	Tekniska skydd	Borås Chalmers KTH Uppsala	4
Biometri	Tekniska skydd	Chalmers Halmstad Karolinska Luleå Stockholm Umeå	6
Forensik	Tekniska skydd	Blekinge Stockholm	2
Intrångsdetektering	Tekniska skydd	FOI Karlstad Luleå	3

Delområde	Kategori	Forskande organisationer	#
Kryptografi	Tekniska skydd	ABB Blekinge Borås Chalmers Ericsson Karlstad Kristianstad KTH Linköping Linné Luleå Lund Mitt SICS Stockholm Uppsala	16
Lägesuppfattning[32]	Tekniska skydd	FOI Skövde	2
Mjukvara	Tekniska skydd	Blekinge Chalmers GU KTH Lund Mälardalen Skövde	7
Åtkomstkontroll	Tekniska skydd	ABB Chalmers Ericsson Karlstad KTH Linköping Luleå SICS Uppsala Örebro	10

Samtliga delområdesnamn ska tolkas med avgränsningen i avsnitt 1.1.3 åtanke. Till exempel innefattar delområdet artificiell intelligens här bara de tillämpningar av artificiell intelligens som har bäring på säkerheten i datorsystem. Mjukvara är ett annat exempel och där ingår inte generell mjukvaruutveckling utan enbart aspekter som bidrar till säkrare (eller mindre säker) mjukvara.

Vissa delområden har ett bredare omfång än andra. Till exempel omfattar *diverse angrepp* alla angrepp utom de som de forskas så mycket på att de förtjänar egna delområden (*nätfiske, cybermobbning, skadlig kod* och *överbelastningsangrepp*). Det kan noteras att *nätfiske* är den enda typ av social engineering som nämns i artiklarna i någon större utsträckning. Ett annat delområde som omfattar mycket är *kryptografi.* Ytterligare ett är *nätverk* som inkluderar allt nätverkssäkerhets-relaterat (exempelvis säkerhetsaspekter av routing, eller säkra kommunikationsprotokoll) som inte omfattas av övriga specifika nätverksdelområden. *Personlig integritet* är också ett delområde som omfattar mycket och likställs ibland med det övergripande säkerhetsbegreppet.

Vissa delområden är snarlika, men har ändå en egen benämning. *Inbyggda system, cyberfysiska system, resursbegränsade enheter, sakernas internet* samt

[32] *Lägesuppfattning* räknas här som tekniskt skydd med tanke på skapandet av lägesuppfattning till stor del är beroende av tekniska system.

trådlösa sensornätverk överlappar till exempel till stor del men förtjänar ändå egna delområden för att visa på de olika organisationernas olika inriktning. Även *utbildning* och *träning* är snarlika men utgör ändå egna delområden. Det bör vidare noteras att till exempel *kultur* och *tillit* inte nödvändigtvis utgör skydd (även om de klassificeras som administrativa skydd här). Rätt säkerhetskultur och rätt nivå av tillit bidrar positivt till säkerheten, men en dålig säkerhetskultur eller alltför låg eller hög tillit är istället negativt för säkerheten. I andra fall har en del nyckelord lagts samman till ett enda delområde. *Åtkomstkontroll* har till exempel de underliggande identifiering, autentisering och auktorisation eller för den delen specifik teknik som lösenord. Å andra sidan förtjänar *biometri* ett eget delområde eftersom det nämns så ofta, på många sätt skiljer sig från traditionell åtkomstkontroll och dessutom kan användas till annat än bara det. *Kryptografi* är av liknande skäl ett eget delområde.

Några ytterligare delområden kräver en förklaring. *Risk* är ett delområde som här täcker in hot-, risk- och sårbarhetsbedömningar – en stor del av planeringsprocessen för att uppnå säkerhet. *Mjukvara* täcker in säker mjukvaruutveckling, inklusive säkra programmeringsspråk, informationsflöden, reverse engineering och sårbarheter. Dock inte *skadlig kod* som står som ett eget delområde. *Anomalidetektering* har ett stort omfång och inkluderar till exempel en del tekniker som ligger nära *intrångsdetektering* samt försök att förhindra angrepp genom att studera potentiella angripares sätt att uttrycka sig lingvistiskt.

Tabell 64 sammanställer vilka organisationer som forskar om vilka kategorier (exklusive domäner för tillämpning som inte lämpar sig för denna typ av summering). Som kan utläsas från tabellens sista kolumn finns det fem organisationer som publicerat sig inom samtliga av fem inkluderade kategorier: Blekinge tekniska högskola, Chalmers tekniska högskola, KTH, Luleå tekniska universitet och Örebro universitet.

Tabell 64 – Vilka organisationer som forskar om vilka delområdeskategorier (Admin. skydd = Administrativa skydd; Angrepp; Hv-nära = Hårdvarunära aspekter; Nät. = Nätverk; Tk. skydd = Tekniska skydd). Om organisationen publicerat inom kategorin visas det med symbolen ●. Vidare anges hur många kategorier varje organisation forskar inom (#). Kategorin domäner för tillämpning inkluderas inte här.

Org.	Admin. skydd	Angrepp	Hv-nära	Nät.	Tk. skydd	#
ABB	●		●	●	●	4
Blekinge	●	●	●	●	●	5
Borås				●	●	2
Chalmers	●	●	●	●	●	5
Ericsson		●	●	●	●	4
FHS	●					1
FOI	●	●		●	●	4
GU		●		●	●	3
Halmstad					●	1
Karlstad	●	●		●	●	4
Karolinska					●	1
Kristianstad					●	1
KTH	●	●	●	●	●	5
Linköping		●	●	●	●	4
Linné	●				●	2
Luleå	●	●	●	●	●	5
Lund	●				●	2
Malmö	●	●	●			3
Mitt	●				●	2
Mälardalen			●	●	●	3
Saab					●	1
SICS			●	●	●	3

Org.	Admin. skydd	Angrepp	Hv-nära	Nät.	Tk. skydd	#
Skövde	●	●			●	3
SP				●		1
Stockholm	●		●	●	●	4
Umeå			●	●	●	3
Uppsala		●	●	●	●	4
Volvo	●				●	2
Örebro	●	●	●	●	●	5
Antal org.	16	13	14	18	26	-

3.3.2 Delområdena och söktermerna

Söktermer (se bilaga 1) låg till grund för söksträngen som användes för att erhålla de artiklar vars nyckelord gav upphov till delområdena. Det kan därför vara av intresse att jämföra delområdena med söktermerna. På så vis kan söktermer som inte täcks in av delområden identifieras – det vill säga söktermer som inte resulterade i något relevant. En del söktermer är på alltför övergripande nivå, eller utgör enbart en variant av en annan sökterm, för att tas med i analysen här. Av de övriga söktermerna (översatta i denna text) som inte uttryckligen finns med som delområde, finns en del som trots allt inkluderas i ett delområde. Detta beskrivs vidare i listan nedan (* betecknar att det följer ett godtyckligt antal godtyckliga bokstäver):

- *Hot, sårbarhet* och *incident* ingår, beroende på exakt sammanhang, antingen i *risk* eller *diverse angrepp*.
- *Anonym**[33] ingår i delområdet *personlig integritet.*
- *Social engineering* är snarlikt delområdet *nätfiske.*
- *Certif** (som i PKI-certifikat) ingår i delområdet *kryptografi.*
- *Pålitliga plattformar* och *manipulationsskydd* räknas också främst som *kryptografi.*

[33] Söktermen *Anonym** hittar allt som inleds med *Anonym* som till exempel Anonymitet, Anonyma, Anonymisering.

- *Kritisk infrastruktur, SCADA* och *smarta elnät* är snarlika *cyberfysiska system.*
- *Spionprogram* ingår i delområdet *skadlig kod*.
- *Juridik* och *datorbrott* förekom begränsat och räknas främst bland *forensik*, men också i förekommande fall bland *cybermobbning* och *diverse angrepp*.
- Något uppenbart delområde för *loggning* och *revision* finns inte, men *lägesuppfattning* tangerar dem delvis.

3.3.3 Trender

Det finns ett antal delområden som verkar ha utvecklats de senaste åren med tanke på att de helt, eller åtminstone i stort sett, saknas i tidigare genomgångar av området. Mest uppenbart är *sakernas internet* som många av de nu inventerade organisationerna forskar om. Närliggande delområden är *positionsinformation, trådlösa sensornätverk, cyberfysiska system, virtualisering, molnet* och *resursbegränsade enheter* vilka nämns i en nyligen genomförd trendspaning (Dam (red.), 2017) av ett urval nya och kommande tekniker med potential *”inom försvaret på 10–25 års sikt”*. Ett annat närliggande delområde som dock inte nämns i tidigare genomgångar är *lägesuppfattning* och det får fortfarande begränsat fokus (se avsnitt 3.3.4). *Artificiell intelligens* och *anomalidetektering* har visserligen forskats om tidigare, men verkar vara på frammarsch. Forskning om *kultur, sociala nätverk* samt *cybermobbning* verkar också ha blivit modernt de senaste fem åren. Forskning om spam har visserligen funnits länge (och är inte uttryckligen med i resultatet utan ingår i *diverse angrepp*), men *nätfiske* är ett i stort sett nytt delområde som dock fortfarande får begränsat fokus (se avsnitt 3.3.4).

3.3.4 Ovanlig forskning

Delområden som få organisationer forskat om i någon större utsträckning och som inte är snarlika andra delområden, kan utgöra särskilda kompetenser hos de organisationer som forskat om dem. Karlstads universitet är till exempel ensamt om att studera *elektronisk röstning* i någon större utsträckning, medan Stockholm är den enda organisation som forskat ordentligt om *forensik.* Tabell 65 visar samtliga ovanliga forskningsinsatser. Direkt efter organisationsnamnet följer antalet artiklar organisationen publicerat inom delområdet, följt av en parentes med den andel detta utgör av organisationens totala forskning. Bara organisationer med minst fyra artiklar inom delområdet har tagits med.

Tabell 65 – Ovanliga delområden och vilka som forskat inom dessa. Det första talet efter varje organisation anger antalet artiklar organisationen publicerat inom delområdet medan procentsatserna anger hur stor andel det antalet utgör av organisationens alla här inkluderade artiklar.

Område	**Organisation/-er och deras antal (andel)**
Elektronisk röstning	Karlstad: 7 *(13 %)*
Forensik	Stockholm: 6 *(16 %)*
Lägesuppfattning	FOI: 5 *(11 %)*
Militär	FHS: 7 *(88 %)* samt FOI: 5 *(11 %)*
Nätfiske	KTH: 5 *(2 %)*
Positionsinformation	Chalmers: 5 *(4 %)* samt KTH: 6 *(3 %)*
Virtualisering	KTH: 7 *(3 %)* samt SICS: 5 *(10 %)*

Det kan noteras att flera av organisationerna som bedriver ovanlig forskning inte samarbetar med de andra inventerade organisationerna i någon större utsträckning (se avsnitt 3.1.2). Mest utmärkande med låg samarbetsgrad är Karlstads universitet, Stockholms universitet, Försvarshögskolan samt Chalmers tekniska högskola. Detta kan vara en del av förklaringen till att deras speciella kunskap inte kunnat spridas till forskare vid andra organisationer (och blivit mindre ovanlig). Med andra ord kan nischen ha bibehållits snarare än spridits. En annan organisation utan samarbeten är Högskolan i Halmstad. De producerar relativt många artiklar och har ett ganska snävt fokus även om andra också forskar inom samma områden. SICS å andra sidan har stor del samarbeten, inklusive med KTH som de delar kompetens inom *virtualisering* och en artikel om delområdet författade de tillsammans.

3.3.5 Vad FOI inte forskar om

FOI:s forskningsartiklar har främst ett *militärt* fokus snarare än ett på *hälsa, fordon, safety, industri, elektronisk röstning* eller *personlig integritet*.

En stor andel av artiklarna är inriktade på de administrativa skydden *träning* (som är snarlikt *utbildning*), *kultur, risk* och *regelefterlevnad* men däremot inte *tillit.*

Artiklarna beskriver *diverse angrepp* i allmänhet, men inte i någon större utsträckning de specifika angreppen *cybermobbning, nätfiske, överbelastningsangrepp* eller *skadlig kod*.

Vad gäller tekniska skydd fokuserar artiklarna på *intrångsdetektering*, *anomalidetektering* och *lägesuppfattning*, men inte på *artificiell intelligens*, *forensik*, *åtkomstkontroll*, *mjukvara*, *kryptografi* eller *biometri*.

Artiklarna fokuserar på *sociala nätverk* men inte på *molnet*, *positionsinformation* eller *nätverk* i allmänhet.

Artiklarna beskriver inte i någon större utsträckning de hårdvarunära aspekterna *inbyggda system*, *virtualisering*, *cyberfysiska system*, *resursbegränsade enheter*, *sakernas internet*, *trådlösa sensornätverk* och *mobiler*.

4 Slutsatser och framtida inventeringar

Operationer i cyberdomänen är ett brett forskningsområde med fokus på antagonistiska hot mot framförallt sammankopplade datorer. Den svenska forskningen som inventerats i rapporten visar att många universitet och högskolor samt ett fåtal forskningsinstitut och företag forskar inom området. Det finns en stor spridning vad gäller i vilken utsträckning de olika organisationerna publicerar forskningsartiklar och det är många artikelförfattare som varit inblandade. Forskningsartiklarna publiceras i en lång rad olika publikationer och vissa publikationer har mer påverkan än andra. Vidare varierar antalet andra artiklar som citerar de inventerade artiklarna och organisationerna har typiskt enbart några enstaka artiklar som är högfrekvent citerade. Organisationerna samarbetar en del med varandra men det finns också utrymme för ytterligare samarbeten, vilket kan sprida kunskap mellan organisationerna, inte minst när det gäller delområden där en enstaka organisation står för den största delen av forskningen. Det finns också många medförfattare från utländska organisationer.

Liknande inventeringar har gjorts tidigare även om de varit mindre omfattande. Från de tidigare genomgångarna kan dock denna rapports inventering visa på trender där vissa delområden nu fått mer uppmärksamhet. Här märks framförallt delområdena sakernas internet, trådlösa sensornätverk, molnet, resursbegränsade enheter, kultur, sociala nätverk och cybermobbning. Artificiell intelligens och anomalidetektering är också mer populära nu om än i något mindre utsträckning. I ännu mindre utsträckning gäller detta lägesuppfattning och nätfiske.

Som komplettering till studien av forskningsartiklar har organisationernas egna forskningspresentationer på deras webbplatser undersökts. Dessa presentationer stämmer inte alltid överens med den bild som ges av artiklarna, vilket kan bero på att presentationerna är framåtblickande och visionära, medan artiklarna visar på tidigare genomförd forskning.

En särskild jämförelse mellan vad FOI:s forskningsartiklar handlar om och vad de andra organisationernas forskningsartiklar rör har också gjorts. En observation är att FOI har ett tydligt militärt fokus, medan de flesta andra istället fokuserar på domäner som hälsa, industriella tillämpningar samt personlig integritet. FOI:s artiklar handlar i första hand om administrativa skydd men också tekniska skydd som intrångsdetektering, anomalidetektering och lägesuppfattning, men inte kryptografi, biometri, åtkomstkontroll och forensik. Hårdvarunära aspekter tar FOI däremot inte upp i någon större utsträckning och inte heller molnet, eller specifika angrepp som skadlig kod och överbelastningsangrepp.

Forskningsområdet förändras snabbt och för att följa utvecklingen vore det lämpligt att varje eller vartannat år göra liknande inventeringar som den som presenteras i denna rapport. Tidigare genomgångar har gjorts men i huvudsak med många år emellan och med olika metoder vilket begränsar möjligheterna till

jämförelser. Det är också möjligt att göra en internationell inventering där inte bara svensk forskning inkluderas. Då kan svensk forskning sättas i ett större sammanhang och globala trender skönjas. En sådan inventering måste dock avgränsas på andra sätt än den här inventeringen för att inte bli alltför omfattande. En möjlighet är att bara sammanställa forskningsartiklar som i sig utgör genomgångar av forskningsartiklar. En annan möjlighet är att koncentrera sig på de mest prestigefyllda tidskrifterna. Vidare kan länder som av olika skäl är mest intressanta ur ett svenskt perspektiv särskilt studeras. Slutligen kan fokus på det operativa ytterligare stärkas och begränsa inventeringen till mognare forskning som går att tillämpa i närtid snarare än mer långsiktigt.

5 Referenser

Referenslistan ges i flera delar. Under denna rubrik kommer först (5.1) allmänna referenser som inte ingår i själva inventeringen. Sedan ges länkar till de tjugo publikationer där flest artiklar publicerats (5.2). Därefter listas länkarna till organisationernas webbplatser i avsnitt 5.3, medan de mest citerade artiklarna återfinns som referenser i avsnitt 5.4.

Dessutom finns i bilaga 2 en komplett lista på alla forskningsartiklar som inventeringen identifierat.

5.1 Allmänna referenser

Agarwal, A., et al. Bibliometrics: tracking research impact by selecting the appropriate metrics, invited review, Asian Journal of Andrology, 2016.

Dam, M. (red.). Trend Analysis Information Security, KTH, 2017.

Fritsch, L., et al. Applications of privacy and security technologies for the protection of personal data in militarily relevant technologies such as IoT, smart environment and digital communications. Trendspaning report for FOI Totalförsvarets forskningsinstitut, Stockholm, Technical report LOF2017-4, Karlstad universitet, 2017.

Förenta Nationerna, United Nations, Department of Economic and Social Affairs, Population Division (2017). World Population Prospects: The 2017 Revision, DVD Edition, via https://esa.un.org/unpd/wpp/DVD/Files/1_Indicators%20(Standard)/EXCEL_FILES/1_Population/WPP2017_POP_F01_1_TOTAL_POPULATION_BOTH_SEXES.xlsx

Försvarsmakten. Militärstrategisk doktrin – MSD 16, 2016.

Försvarsmakten. Inriktning av Försvarsmaktens plan för forskning och teknikutveckling, FM2016-23660:3, 2018.

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

Högskolelag (1992:1434), via Regeringskansliets rättsdatabaser, http://rkrattsbaser.gov.se/sfst?bet=1992:1434

Isenberg, P., et al., Visualization as Seen Through its Research Paper Keywords, IEEE Transactions on Visualization and Computer Graphics, vol. 23:1, 2017.

Joint Chiefs of Staff, Joint Publication 3-12 (R), Cyberspace Operations, 2013.

Karlsson, F., et al. En genomgång av informationssäkerhetsforskning i Sverige. Handelshögskolan, Örebro universitet, 2011.

Kuehl, D.T.. From Cyberspace to Cyberpower: Defining the Problem, i Cyberpower and National Security, National Defense University Press, 2009.

Löfvenberg, J. En översikt över IT-säkerhetsforskning i Sverige, FOI-R--3069--SE, 2010.

Oxford Living Dictionaries, Oxford University Press, 2018, via https://en.oxforddictionaries.com/definition/operation

Post- och telestyrelsen. Bilaga 4 - Kartläggning av forskning inom IT-säkerhet i Sverige, i Tillit till IT vid Internetanvändning, Förutsättningar för att följa utvecklingen – indikatorer och svensk forskning inom IT-säkerhet, PTS-ER-2002:24, 2002.

Regeringskansliet. Nationell strategi för samhällets informations- och cybersäkerhet. Skr. 2016/17:213, Regeringskansliet 2017.

Svenska Akademien. Svensk ordbok, 2009, via https://svenska.se

Universitetskanslersämbetet, Var finns universiteten och högskolorna?, 2018, https://www.uka.se/fakta-om-hogskolan/universitet-och-hogskolor/var-finns-universiteten-och-hogskolorna-.html

von Sydow, B., et al. Forskning och utveckling på försvarsområdet, Betänkande av Försvarsforskningsutredningen, Statens offentliga utredningar, SOU 2016:90, 2016.

5.2 Länkar till de vanligaste publikationerna

Publikation	Länk
L Notes in Computer Science/AI/Bioinformatics	https://www.springer.com/gp/computer-science/lncs
IFIP Advances in Information and Comm Tech	https://link.springer.com/bookseries/6102
ACM Intl Conference Proceeding Series	https://www.acm.org/publications/icps-series
Computers and Security	https://www.journals.elsevier.com/computers-and-security
Communications in Computer and Info Science	http://www.springer.com/series/7899

Publikation	Länk
Information and Computer Security	http://emeraldgrouppublishing.com/products/journals/journals.htm?id=ics
ACM Conference on Computer and Comm Security	https://www.sigsac.org/ccs/CCS2018/papers/
L Notes Institute Comp Sci, Soc-Informatics & Telecom	http://www.springer.com/series/8197
Annual Hawaii International Conf on System Sci	https://hicss.hawaii.edu/
Security and Communication Networks	https://www.hindawi.com/journals/scn/
Procedia Computer Science	https://www.journals.elsevier.com/procedia-computer-science
Intl Symp on Human Aspects of Info Sec & Assurance	http://www.haisa.org/
IFAC-PapersOnLine	https://www.journals.elsevier.com/ifac-papersonline/
Future Generation Computer Systems	https://www.journals.elsevier.com/future-generation-computer-systems
IEEE Transactions on Dependable and Secure Comp	https://www.computer.org/web/tdsc
European Intelligence and Security Informatics Conf	http://www.eisic.eu/
Computers in Human Behavior	https://www.journals.elsevier.com/computers-in-human-behavior
Advances in Intelligent Systems and Computing	http://www.springer.com/series/11156

5.3 Länkar till organisationernas webbplatser

Referens	Länk
ABB, 2018	http://you.abb.com/en/insight/
BTH, 2018a	https://www.bth.se/eng/research/computer-science-and-engineering/bonseyes/
BTH, 2018b	https://www.bth.se/eng/research/computer-science-and-engineering/agilesec/
HB, 2018	http://www.hb.se/Forskning/Forskningsportal/Forskare/Salomonson-Nicklas/
CTH, 2018a	https://www.chalmers.se/sv/institutioner/cse/organisation/is/Sidor/default.aspx
CTH, 2018b	https://www.chalmers.se/sv/institutioner/cse/organisation/ns/Sidor/default.aspx
CTH, 2018c	https://www.chalmers.se/sv/personal/Sidor/olafl.aspx
CTH, 2018d	https://www.chalmers.se/sv/personal/Sidor/lbei.aspx
Ericsson, 2018a	https://www.ericsson.com/en/security/sics
Ericsson, 2018b	https://www.ericsson.com/en/security/concordia
FOI, 2018a	https://www.foi.se/var-kunskap/informationssakerhet-och-kommunikation/informationssakerhet.html
FOI, 2018b	https://www.foi.se/var-kunskap/systemutveckling-och-human-factors/manniska-teknik-och-organisation-mto.html
FOI, 2018c	https://www.foi.se/var-kunskap/sakerhetspolitik/nordeuropeisk-och-transatlantisk-sakerhet/experter.html
FOI, 2018d	https://www.foi.se/var-kunskap/beslutsstodssystem-och-informationsfusion/beslutsstod-kunskapshantering-och-informationsfusion.html

Referens	Länk
FOI, 2018e	https://www.foi.se/var-kunskap/informationssakerhet-och-kommunikation/it-forensik.html
GU, 2018	https://www.gu.se/omuniversitetet/enheter/?departmentId=107833#tabContentAnchor2
KAU, 2018	https://www.kau.se/cs/forskning/forskningsomraden/datasakerhet-personlig-integritet-prisec/prisec-privacy-and-security
KTH, 2018a	https://www.kth.se/nse/research
KTH, 2018b	https://www.kth.se/sv/ise/research/privacy-and-security/privacy-and-security-1.686028).
LIU, 2018a	https://liu.se/en/organisation/liu/ida/adit
LIU, 2018b	http://people.isy.liu.se/jalar/qkg/ceniit.html
LIU, 2018c	https://liu.se/en/organisation/liu/ida/adit
LNU, 2018	https://lnu.se/forskning/sok-forskning/forskningsprojekt/provably-secure-self-protecting-systems-prosses/
LTU, 2018a	https://www.ltu.se/research/subjects/information-systems/
LTU, 2018b	https://www.ltu.se/research/subjects/information-systems/Informationssakerhet
LU, 2018a	http://www.risk.lth.se/research/
LU, 2018b	http://portal.research.lu.se/portal/sv/organisations-researchgroups/networks-and-security(e7a79d6c-a80e-4bd4-8de0-28642c89e38b).html
MDH, 2018	http://www.es.mdh.se/research-groups/26-Data_Communication
SICS, 2018a	https://www.sics.se/groups/security-lab-sec
SICS, 2018b	https://www.swedishict.se/competence-areas/rise-centre-for-cybersecurity

Referens	Länk
HS, 2018	http://www.his.se/Forskning/informationsteknologi/Informationssystem/KLISTER/
SP, 2018a	https://www.sp.se/sv/press/Sidor/experts.aspx
SP, 2018b	https://www.sp.se/sv/index/research/dependable_systems/safecer/Sidor/default.aspx
SU, 2018	https://dsv.su.se/en/research/research-areas/security
UU, 2018	http://www.it.uu.se/research/arenas/security?lang=en
ORU, 2018a	https://www.oru.se/forskning/forskningsprojekt/fp/?rdb=p1146
ORU, 2018b	https://www.oru.se/forskning/forskningsprojekt/fp/?rdb=p1833

5.4 De mest citerade artiklarna

Antinyan V., Staron M., Meding W., Österström P., Wikström E., Wranker J., Henriksson A., Hansson J. Identifying risky areas of software code in Agile/Lean software development: An industrial experience report. 2014 Software Evolution Week - IEEE Conference on Software Maintenance, Reengineering, and Reverse Engineering, CSMR-WCRE 2014 - Proceedings, 2014.

Baca D., Petersen K. Countermeasure graphs for software security risk assessment: An action research. Journal of Systems and Software, vol. 86:9, 2013.

Beckman L., Hagquist C., Hellström L. Discrepant gender patterns for cyberbullyiyng and traditional bullying - An analysis of Swedish adolescent data. Computers in Human Behavior, vol. 29:5, 2013.

Broberg N., Van Delft B., Sands D. Paragon for practical programming with information-flow control. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8301 LNCS, 2013.

Cao Z., Zhang S., Ji X., Zhang L. Secure random linear network coding on a wiretap network. AEU - International Journal of Electronics and Communications, vol. 69:1, 2014.

Christin D., Roßkopf C., Hollick M., Martucci L.A., Kanhere S.S. IncogniSense: An anonymity-preserving reputation framework for participatory sensing applications. Pervasive and Mobile Computing, vol. 9:3, 2013.

Cohen K., Johansson F., Kaati L., Mork J.C. Detecting Linguistic Markers for Radical Violence in Social Media. Terrorism and Political Violence, vol. 26:1, 2014.

Conti M., Dragoni N., Lesyk V. A Survey of Man in the Middle Attacks. IEEE Communications Surveys and Tutorials, vol. 18:3, 2016.

Da Silva J.M.B., Jr., Fodor G., Maciel T.F. Performance analysis of network-assisted two-hop D2D communications. 2014 IEEE Globecom Workshops, GC Wkshps 2014, 2014.

Derhamy H., Eliasson J., Delsing J., Priller P. A survey of commercial frameworks for the Internet of Things. IEEE International Conference on Emerging Technologies and Factory Automation, ETFA, Vol. 2015-October, 2015.

Ebadi H., Sands D., Schneider G. Differential privacy: Now it's getting personal. Conference Record of the Annual ACM Symposium on Principles of Programming Languages, Vol. 2015-January, 2015.

Fischer-Hübner S., Angulo J., Pulls T. How can cloud users be supported in deciding on, tracking and controlling how their data are used?. IFIP Advances in Information and Communication Technology, Vol. 421, 2014.

Flores W.R., Holm H., Nohlberg M., Ekstedt M. Investigating personal determinants of phishing and the effect of national culture. Information and Computer Security, vol. 23:2, 2015.

Franke U., Brynielsson J. Cyber situational awareness - A systematic review of the literature. Computers and Security, Vol. 46, 2014.

Ghazawneh A., Henfridsson O. Balancing platform control and external contribution in third-party development: The boundary resources model. Information Systems Journal, vol. 23:2, 2013.

Gholami A., Lind A.-S., Reichel J., Litton J.-E., Edlund A., Laure E. Privacy threat modeling for emerging biobankclouds. Procedia Computer Science, Vol. 37, 2014.

Guo Q., Johansson T., Löndahl C. Solving LPN using covering codes. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8873, 2014.

Guo Q., Johansson T., Stankovski P. A key recovery attack on MDPC with CCA security using decoding errors. Lecture Notes in Computer Science (including

subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10031 LNCS, 2016.

Hedin D., Birgisson A., Bello L., Sabelfeld A. JSFlow: Tracking information flow in JavaScript and its APIs. Proceedings of the ACM Symposium on Applied Computing, 2014.

Hedin D., Bello L., Sabelfeld A. Value-Sensitive Hybrid Information Flow Control for a JavaScript-Like Language. Proceedings of the Computer Security Foundations Workshop, Vol. 2015-September, 2015.

Hedström K., Karlsson F., Kolkowska E. Social action theory for understanding information security non-compliance in hospitals the importance of user rationale. Information Management and Computer Security, vol. 21:4, 2013.

Heickerö R. Cyber Terrorism: Electronic Jihad. Strategic Analysis, vol. 38:4, 2014.

Hendrickx J.M., Johansson K.H., Jungers R.M., Sandberg H., Sou K.C. Efficient computations of a security index for false data attacks in power networks. IEEE Transactions on Automatic Control, vol. 59:12, 2015.

Hofbauer H., Alonso-Fernandez F., Wild P., Bigun J., Uhl A. A ground truth for Iris segmentation. Proceedings - International Conference on Pattern Recognition, 2014.

Huang X., Craig P., Wang Q. Identity-based association protocols for wireless personal area networks. Proceedings - 15th IEEE International Conference on Computer and Information Technology, CIT 2015, 14th IEEE International Conference on Ubiquitous Computing and Communications, IUCC 2015, 13th IEEE International Conference on Dependable, Autonomic and Secure Computing, DASC 2015 and 13th IEEE International Conference on Pervasive Intelligence and Computing, PICom 2015, 2015.

Hummen R., Ziegeldorf J.H., Shafagh H., Raza S., Wehrle K. Towards viable certificate-based authentication for the Internet of Things. HotWiSec 2013 - Proceedings of the 2013 ACM Workshop on Hot Topics on Wireless Network Security and Privacy, 2013.

Hummen R., Shafagh H., Raza S., Voig T., Wehrle K. Delegation-based authentication and authorization for the IP-based Internet of Things. 2014 11th Annual IEEE International Conference on Sensing, Communication, and Networking, SECON 2014, 2014.

Islam M.M., Lautenbach A., Sandberg C., Olovsson T. A risk assessment framework for automotive embedded systems. CPSS 2016 - Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security, Co-located with Asia CCS 2016, 2016.

Jacobsson A., Davidsson P. Towards a model of privacy and security for smart homes. IEEE World Forum on Internet of Things, WF-IoT 2015 - Proceedings, 2015.

Jacobsson A., Boldt M., Carlsson B. A risk analysis of a smart home automation system. Future Generation Computer Systems, Vol. 56, 2016.

Jonsson L.S., Priebe G., Bladh M., Svedin C.G. Voluntary sexual exposure online among Swedish youth - Social background, Internet behavior and psychosocial health. Computers in Human Behavior, Vol. 30, 2014.

Kajtazi M., Bulgurcu B. Information security policy compliance: An empirical study on escalation of commitment. 19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime, Vol. 3, 2013.

Kang K., Pang Z., Xu L.D., Ma L., Wang C. An interactive trust model for application market of the internet of things. IEEE Transactions on Industrial Informatics, vol. 10:2, 2014.

Kolkowska E., Dhillon G. Organizational power and information security rule compliance. Computers and Security, Vol. 33, 2013.

Laxhammar R., Falkman G. Online learning and sequential anomaly detection in trajectories. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 36:6, 2014.

Le A., Loo J., Lasebae A., Vinel A., Chen Y., Chai M. The impact of rank attack on network topology of routing protocol for low-power and lossy networks. IEEE Sensors Journal, vol. 13:10, 2013.

Lindh M., Nolin J. Information We Collect: Surveillance and Privacy in the Implementation of Google Apps for Education. European Educational Research Journal, vol. 15:6, 2016.

Mikaelyan A., Alonso-Fernandez F., Bigun J. Periocular recognition by detection of local symmetry patterns. Proceedings - 10th International Conference on Signal-Image Technology and Internet-Based Systems, SITIS 2014, 2015.

Mohd B.J., Hayajneh T., Vasilakos A.V. A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues. Journal of Network and Computer Applications, Vol. 58, 2015.

Nawareg M., Muhammad S., Amselem E., Bourennane M. Experimental Measurement-Device-Independent Entanglement Detection. Scientific Reports, Vol. 5, 2015.

Paladi N., Michalas A. 'One of our hosts in another country': Challenges of data geolocation in cloud storage. 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and

Electronic Systems, VITAE 2014 - Co-located with Global Wireless Summit, 2014.

Pang Z., Chen Q., Tian J., Zheng L., Dubrova E. Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things. International Conference on Advanced Communication Technology, ICACT, 2013a.

Pang Z., Yu K., Åkerberg J., Gidlund M. An RTOS-based architecture for industrial wireless sensor network stacks with multi-processor support. Proceedings of the IEEE International Conference on Industrial Technology, 2013b.

Pang Z., Zheng L., Tian J., Kao-Walter S., Dubrova E., Chen Q. Design of a terminal solution for integration of in-home health care devices and services towards the Internet-of-Things. Enterprise Information Systems, vol. 9:1, 2015.

Priebe G., Mitchell K.J., Finkelhor D. To tell or not to tell? Youth's responses to unwanted internet experiences. Cyberpsychology, vol. 7:1, 2013.

Pulls T., Peeters R., Wouters K. Distributed privacy-preserving transparency logging. Proceedings of the ACM Conference on Computer and Communications Security, 2013.

Pöhls H.C., Angelakis V., Suppan S., Fischer K., Oikonomou G., Tragos E.Z., Rodriguez R.D., Mouroutis T. RERUM: Building a reliable IoT upon privacy- and security- enabled smart objects. 2014 IEEE Wireless Communications and Networking Conference Workshops, WCNCW 2014, 2014.

Ray A., Åkerberg J., Björkman M., Gidlund M. POSTER: An approach to assess security, capacity and reachability for heterogeneous industrial networks. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, Vol. 164, 2015.

Ray A., Akerberg J., Bjorkman M., Gidlund M. Future research challenges of secure heterogeneous industrial communication networks. IEEE International Conference on Emerging Technologies and Factory Automation, ETFA, Vol. 2016-November, 2016.

Raza S., Shafagh H., Hewage K., Hummen R., Voigt T. Lithe: Lightweight secure CoAP for the internet of things. IEEE Sensors Journal, vol. 13:10, 2013a.

Raza S., Wallgren L., Voigt T. SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Networks, vol. 11:8, 2013b.

Raza S., Seitz L., Sitenkov D., Selander G. S3K: Scalable Security with Symmetric Keys - DTLS Key Establishment for the Internet of Things. IEEE Transactions on Automation Science and Engineering, vol. 13:3, 2016.

Sandberg H., Amin S., Johansson K.H. Cyberphysical security in networked control systems: An introduction to the issue. IEEE Control Systems, vol. 35:1, 2015.

Shokri R., Theodorakopoulos G., Papadimitratos P., Kazemi E., Hubaux J.-P. Hiding in the mobile crowd: Location privacy through collaboration. IEEE Transactions on Dependable and Secure Computing, vol. 11:3, 2014.

Shu Z., Wan J., Li D., Lin J., Vasilakos A.V., Imran M. Security in Software-Defined Networking: Threats and Countermeasures. Mobile Networks and Applications, vol. 21:5, 2016.

Sigholm J., Bang M. Towards Offensive cyber counterintelligence: Adopting a target-centric view on advanced persistent threats. Proceedings - 2013 European Intelligence and Security Informatics Conference, EISIC 2013, 2013.

Simplicio Jr. M.A., De Oliveira B.T., Margi C.B., Barreto P.S.L.M., Carvalho T.C.M.B., Näslund M. Survey and comparison of message authentication solutions on wireless sensor networks. Ad Hoc Networks, vol. 11:3, 2013.

Slonje R., Smith P.K., Frisén A. The nature of cyberbullying, and strategies for prevention. Computers in Human Behavior, vol. 29:1, 2013.

Soderberg A., Johansson R. Safety contract based design of software components. 2013 IEEE International Symposium on Software Reliability Engineering Workshops, ISSREW 2013, 2013.

Sommestad T., Ekstedt M., Holm H. The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures. IEEE Systems Journal, vol. 7:3, 2013.

Sommestad T., Hallberg J., Lundholm K., Bengtsson J. Variables influencing information security policy compliance: A systematic review of quantitative studies. Information Management and Computer Security, vol. 22:1, 2014.

Sommestad T., Karlzén H., Hallberg J. The sufficiency of the theory of planned behavior for explaining information security policy compliance. Information and Computer Security, vol. 23:2, 2015a.

Sommestad T., Sandström F. An empirical test of the accuracy of an attack graph analysis tool. Information and Computer Security, vol. 23:5, 2015b.

Sou K.C., Sandberg H., Johansson K.H. On the exact solution to a smart grid cyber-security analysis problem. IEEE Transactions on Smart Grid, vol. 4:2, 2013.

Steinhauer H.J., Karlsson A., Andler S.F. Traceable uncertainty. Proceedings of the 16th International Conference on Information Fusion, FUSION 2013, 2013.

Teixeira A., Shames I., Sandberg H., Johansson K.H. A secure control framework for resource-limited adversaries. Automatica, Vol. 51, 2015.

Toghian M., Morogan M.C. Suggesting a method to improve encryption key management in wireless sensor networks. Indian Journal of Science and Technology, vol. 8:19, 2015.

Tragos E.Z., Angelakis V., Fragkiadakis A., Gundlegard D., Nechifor C.-S., Oikonomou G., Pohls H.C., Gavras A. Enabling reliable and secure IoT-based smart city applications. 2014 IEEE International Conference on Pervasive Computing and Communication Workshops, PERCOM WORKSHOPS 2014, 2014.

Wallgren L., Raza S., Voigt T. Routing attacks and countermeasures in the RPL-based internet of things. International Journal of Distributed Sensor Networks, Vol. 2013, 2013.

Wang Y., Min Q., Han S. Understanding the effects of trust and risk on individual behavior toward social media platforms: A meta-analysis of the empirical evidence. Computers in Human Behavior, Vol. 56, 2016.

Winter P., Pulls T., Fuss J. ScrambleSuit: A polymorphic network protocol to circumvent censorship. Proceedings of the ACM Conference on Computer and Communications Security, 2013.

Yu Y., Xue L., Au M.H., Susilo W., Ni J., Zhang Y., Vasilakos A.V., Shen J. Cloud data integrity checking with an identity-based auditing mechanism from RSA. Future Generation Computer Systems, Vol. 62, 2016.

Bilaga 1 – Söksträngen

Den slutliga söksträngen bestod av engelska söktermer baserade på Tabell 66. Varje träff måste antingen matcha någon av termerna i första kolumnen (som rör både cyber och säkerhet samtidigt), alternativt någon av termerna i andra kolumnen (som rör cyber) och samtidigt någon av termerna i tredje kolumnen (som rör säkerhet). * betecknar att det följer ett godtyckligt antal godtyckliga bokstäver, det vill säga söktermen anonym* hittar allt som inleds med anonym som till exempel anonymitet, anonyma och anonymisering.

Tabell 66 – Söktermerna.

Söktermer som rör cyber och säkerhet	**Söktermer som rör cyber**	**Söktermer som rör säkerhet**
information security	artificial intelligence	anomaly detection
biometrics	cloud	anonym*
computer crime	computer	antagonist
computer network attack	cyber*	attack*
computer network defen*	cyber-physical	audit
computer network exploitation	database	authentication
computer network operations	embedded	availability
crypto*	internet	certif*
malware	internet of things	confidentiality
password	IoT	critical infrastructure
software security	programming	defen*
spyware	SCADA	denial of service
trusted platform	smart grids	exploit
	software	forensics
	wireless	incident
	virtual*	integrity

Söktermer som rör cyber och säkerhet	Söktermer som rör cyber	Söktermer som rör säkerhet
		intrusion
		legal
		logging
		logs
		malicious
		military
		offen*
		pre-emptive
		preventive
		privacy
		proactive
		reverse engineering
		risk analysis
		risk management
		secre*
		secur*
		situation awareness
		situation picture
		situational awareness
		situational picture
		social engineering
		tamper
		threat
		trust
		vulnerab*

Vidare inkluderades:

- bara artiklar med minst en författare verksam vid en svensk organisation
- bara artiklar inom något av ämnena datavetenskap, ingenjörsvetenskap, matematik, samhällsvetenskap, företagsekonomi, energi, beslutsteori, ekonomi, psykologi eller multidisciplinärt
- inte artiklar som även är inom något av ämnena medicin, biokemi, materialvetenskap eller miljövetenskap
- bara artiklar publicerade 2012-2018 eller som accepterats för publicering 2018-2019.

Den slutliga söksträngen i sin helhet såg därmed ut som följer:

TITLE-ABS-KEY(“information security” OR malware OR biometrics OR "computer crime" OR "computer network attack" OR "computer network defen*" OR "computer network exploitation" OR "computer network operations" OR crypto* OR password OR "software security" OR spyware OR "trusted platform") OR (TITLE-ABS-KEY("artificial intelligence" OR cloud OR computer OR cyber* OR cyber-physical OR database OR embedded OR internet OR "internet of things" OR IoT OR programming OR SCADA OR "smart grids" OR software OR wireless OR virtual*) AND TITLE-ABS-KEY("anomaly detection" OR anonym* OR antagonist OR attack* OR authentication OR availability OR certif* OR confidentiality OR "critical infrastructure" OR defen* OR "denial of service" OR exploit OR forensics OR incident OR integrity OR intrusion OR legal OR logging OR logs OR malicious OR military OR offen* OR pre-emptive OR preventive OR privacy OR proactive OR "reverse engineering" OR "risk analysis" OR "risk management" OR secre* OR secur* OR "situation awareness" OR "situation picture" OR "situational awareness" OR "situational picture" OR "social engineering" OR tamper OR threat OR trust OR vulnerab*)) AND (LIMIT-TO (AFFILCOUNTRY,"Sweden ")) AND (LIMIT-TO (SUBJAREA,"COMP ") OR LIMIT-TO (SUBJAREA,"ENGI ") OR LIMIT-TO (SUBJAREA,"MATH ") OR LIMIT-TO (SUBJAREA,"SOCI ") OR LIMIT-TO (SUBJAREA,"BUSI ") OR LIMIT-TO (SUBJAREA,"ENER ") OR LIMIT-TO (SUBJAREA,"DECI ") OR LIMIT-TO (SUBJAREA,"ECON ") OR LIMIT-TO (SUBJAREA,"PSYC ") OR LIMIT-TO (SUBJAREA,"MULT ") OR EXCLUDE (SUBJAREA,"MEDI ") OR EXCLUDE (SUBJAREA,"BIOC ") OR EXCLUDE (SUBJAREA,"MATE ") OR EXCLUDE (SUBJAREA,"ENVI ")) AND (LIMIT-TO (PUBYEAR,2019) OR LIMIT-TO (PUBYEAR,2018) OR LIMIT-TO (PUBYEAR,2017) OR LIMIT-TO (PUBYEAR,2016) OR LIMIT-TO (PUBYEAR,2015) OR LIMIT-TO (PUBYEAR,2014) OR LIMIT-TO (PUBYEAR,2013))

Bilaga 2 – Samtliga identifierade forskningsartiklar

Artikel	Organisation/-er
Abdelraheem M.A., Alizadeh J., Alkhzaimi H.A., Aref M.R., Bagheri N., Gauravaram P. Improved linear cryptanalysis of reduced-round SIMON-32 and SIMON-48. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9462, 2015.	SICS
Abdelraheem M.A., Andersson T., Gehrmann C. Searchable encrypted relational databases: Risks and countermeasures. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10436 LNCS, 2017.	Lund
Abdelraheem M.A., Gehrmann C., Lindström M., Nordahl C. Executing Boolean queries on an encrypted Bitmap index. CCSW 2016 - Proceedings of the 2016 ACM Cloud Computing Security Workshop, co-located with CCS 2016, 2016.	Blekinge, Lund
Abdullah N., Håkansson A., Moradian E. Blockchain based approach to enhance big data authentication in distributed environment. International Conference on Ubiquitous and Future Networks, ICUFN, 2017.	KTH, Stockholm
Abdullah N., Kounelis I., Muftic S. Security extensions for mobile commerce objects. SECURWARE 2014 - 8th International Conference on Emerging Security Information, Systems and Technologies, 2014.	KTH
Abidin A., Aly A., Rúa E.A., Mitrokotsa A. Efficient verifiable computation of XOR for biometric authentication. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10052 LNCS, 2016.	Chalmers
Abidin A., Matsuura K., Mitrokotsa A. Security of a privacy-preserving biometric authentication protocol revisited. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8813, 2014.	Chalmers
Abidin A., Mitrokotsa A. Security aspects of privacy-preserving biometric authentication based on ideal lattices and ring-LWE. 2014 IEEE International Workshop on Information Forensics and Security, WIFS 2014, 2015.	Chalmers
Abidin A., Pagnin E., Mitrokotsa A. Attacks on privacy-preserving biometric authentication. Lecture Notes in Computer Science (including	Chalmers

subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8788, 2014.	
Abrahamsson M., Johansson H., Nilsson J., Magnusson S.E. IV. Risk based decision making: Three examples of practical application tools. Topics in Safety, Risk, Reliability and Quality, Vol. 8, 2015.	Lund
Adamov A., Carlsson A. A sandboxing method to protect cloud cyberspace. Proceedings of 2015 IEEE East-West Design and Test Symposium, EWDTS 2015, 2016.	Blekinge
Adamov A., Carlsson A. Cloud incident response model. Proceedings of 2016 IEEE East-West Design and Test Symposium, EWDTS 2016, 2017.	Blekinge
Adamov A., Carlsson A. The state of ransomware. Trends and mitigation techniques. Proceedings of 2017 IEEE East-West Design and Test Symposium, EWDTS 2017, 2017.	Blekinge
Adermon A., Liang C.-Y. Piracy and music sales: The effects of an anti-piracy law. Journal of Economic Behavior and Organization, Vol. 105, 2014.	Uppsala
Afzal Z., Lindskog S. IDS rule management made easy. Proceedings of the 8th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2016, 2017.	Karlstad
Afzal Z., Rossebo J., Talha B., Chowdhury M. A Wireless Intrusion Detection System for 802.11 networks. Proceedings of the 2016 IEEE International Conference on Wireless Communications, Signal Processing and Networking, WiSPNET 2016, 2016.	Karlstad
Agadakos I., Hallgren P., Damopoulos D., Sabelfeld A., Portokalidis G. Location-enhanced authentication using the IoT because you cannot be in two places at once. ACM International Conference Proceeding Series, Vol. 5-9-December-2016, 2016.	Chalmers
Agrawal T.K., Koehl L., Campagne C. Cryptographic tracking tags for traceability in textiles and clothing supply chain. Uncertainty Modelling in Knowledge Engineering and Decision Making - Proceedings of the 12th International FLINS Conference, FLINS 2016, 2016.	Borås
Ahmad I., Kumar T., Liyanage M., Okwuibe J., Ylianttila M., Gurtov A. 5G security: Analysis of threats and solutions. 2017 IEEE Conference on Standards for Communications and Networking, CSCN 2017, 2017.	Linköping
Ahmad I., Liyanage M., Ylianttila M., Gurtov A. Analysis of deployment challenges of Host Identity Protocol. EuCNC 2017 - European Conference on Networks and Communications, 2017.	Linköping
Akalin N., Kiselev A., Kristoffersson A., Loutfi A. An Evaluation Tool of the Effect of Robots in Eldercare on the Sense of Safety and Security. Lecture Notes in Computer Science (including subseries Lecture Notes	Örebro

in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10652 LNAI, 2017.	
Alam Q., Tabbasum S., Malik S.U.R., Alam M., Ali T., Akhunzada A., Khan S.U., Vasilakos A.V., Buyya R. Formal Verification of the xDAuth Protocol. IEEE Transactions on Information Forensics and Security, vol. 11:9, 2016.	Luleå
Alaqra A., Fischer-Hübner S., Groß T., Lorünser T., Slamanig D. Signatures for privacy, trust and accountability in the cloud: Applications and requirements. IFIP Advances in Information and Communication Technology, Vol. 476, 2016.	Karlstad
Alaqra A., Fischer-Hübner S., Pettersson J.S., Wästlund E. Stakeholders' perspectives on malleable signatures in a cloud-based ehealth scenario. Proceedings of the 10th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2016, 2016.	Karlstad
Al-Douri Y.K., Pangracious V., Al-Doori M. Artifical immune system using Genetic Algorithm and decision tree. 2016 International Conference on Bio-Engineering for Smart Technologies, BioSMART 2016, 2017.	Luleå
Alexiou N., Basagiannis S., Petridou S. Formal security analysis of near field communication using model checking. Computers and Security, Vol. 60, 2016.	KTH
Alexiou N., Basagiannis S., Petridou S. Security analysis of NFC relay attacks using probabilistic model checking. IWCMC 2014 - 10th International Wireless Communications and Mobile Computing Conference, 2014.	KTH
Alexiou N., Gisdakis S., Lagana M., Papadimitratos P. Towards a secure and privacy-preserving multi-service vehicular architecture. 2013 IEEE 14th International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2013, 2013.	KTH
Alexiou N., Laganà M., Gisdakis S., Khodaei M., Papadimitratos P. VeSPA: Vehicular security and privacy-preserving architecture. HotWiSec 2013 - Proceedings of the 2013 ACM Workshop on Hot Topics on Wireless Network Security and Privacy, 2013.	KTH
Alobaidli H., Nasir Q., Iqbal A., Guimaraes M. Challenges of cloud log forensics. Proceedings of the SouthEast Conference, ACMSE 2017, 2017.	KTH
Alonso-Fernandez F., Bigun J. A survey on periocular biometrics research. Pattern Recognition Letters, Vol. 82, 2016.	Halmstad
Alonso-Fernandez F., Bigun J. Best regions for periocular recognition with NIR and visible images. 2014 IEEE International Conference on Image Processing, ICIP 2014, 2014.	Halmstad

Alonso-Fernandez F., Bigun J. Fake iris detection: A comparison between near-infrared and visible images. Proceedings - 10th International Conference on Signal-Image Technology and Internet-Based Systems, SITIS 2014, 2015.	Halmstad
Alonso-Fernandez F., Farrugia R.A., Bigun J. Eigen-patch iris super-resolution for iris recognition improvement. 2015 23rd European Signal Processing Conference, EUSIPCO 2015, 2015.	Halmstad
Alonso-Fernandez F., Farrugia R.A., Bigun J. Improving Very Low-Resolution Iris Identification via Super-Resolution Reconstruction of Local Patches. Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI), 2017.	Halmstad
Alonso-Fernandez F., Farrugia R.A., Bigun J. Iris Super-Resolution Using Iterative Neighbor Embedding. IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, Vol. 2017-July, 2017.	Halmstad
Alonso-Fernandez F., Farrugia R.A., Bigun J. Reconstruction of smartphone images for low resolution iris recognition. 2015 IEEE International Workshop on Information Forensics and Security, WIFS 2015 - Proceedings, 2015.	Halmstad
Alonso-Fernandez F., Farrugia R.A., Bigun J. Very low-resolution iris recognition via Eigen-patch super-resolution and matcher fusion. 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems, BTAS 2016, 2016.	Halmstad
Alsabbagh B., Kowalski S. A framework and prototype for a socio-technical security information and event management system (ST-SIEM). Proceedings - 2016 European Intelligence and Security Informatics Conference, EISIC 2016, 2017.	Stockholm
AlSabbagh B., Kowalski S. Security from a systems thinking perspective - Applying soft systems methodology to the analysis of an information security incident. 58th Annual Meeting of the International Society for the Systems Sciences, ISSS 2014, 2014.	Stockholm
Al-Saqaf W. Internet censorship circumvention tools: Escaping the control of the syrian regime. Media and Communication, vol. 4:1, 2016.	Örebro
Amorim J.A., Ahlfeldt R.-M., Gustavsson P.M., Andler S.F. Privacy and security in cyberspace: Training perspectives on the personal data ecosystem. Proceedings - 2013 European Intelligence and Security Informatics Conference, EISIC 2013, 2013.	Saab, Skövde
Andersson D., Rankin A., Diptee D. Approaches to team performance assessment: a comparison of self-assessment reports and behavioral observer scales. Cognition, Technology and Work, vol. 19:43134, 2017.	FOI

Andersson D., Thorstensson M. Reconstruction and exploration: Applications in criminology. Proceedings - 2013 European Intelligence and Security Informatics Conference, EISIC 2013, 2013.	FOI
Andersson M., Khisti A., Skoglund M. Secure key agreement over reciprocal fading channels in the low SNR regime. IEEE Workshop on Signal Processing Advances in Wireless Communications, SPAWC, 2013.	KTH
Andersson M., Schaefer R.F., Oechtering T.J., Skoglund M. Polar coding for bidirectional broadcast channels with common and confidential messages. IEEE Journal on Selected Areas in Communications, vol. 31:9, 2013.	KTH
Andersson M., Svennerlind C., Malmqvist I., Anckarsäter H. New Swedish forensic psychiatric facilities: Visions and outcomes. Facilities, vol. 31:1, 2013.	Chalmers
Angulo J., Wästlund E. Identity management through "profiles": Prototyping an online information segregation service. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 8006 LNCS:PART 3, 2013.	Karlstad
Angulo J., Wästlund E., Högberg J. What would it take for you to tell your secrets to a cloud?: Studying decision factors when disclosing information to cloud services. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8788, 2014.	Karlstad
Antignac T., Sands D., Schneider G. Data minimisation: A language-based approach. IFIP Advances in Information and Communication Technology, Vol. 502, 2017.	Chalmers, Göteborg
Antignac T., Scandariato R., Schneider G. A privacy-aware conceptual model for handling personal data. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9952 LNCS, 2016.	Chalmers
Antinyan V., Staron M., Meding W., Österström P., Wikström E., Wranker J., Henriksson A., Hansson J. Identifying risky areas of software code in Agile/Lean software development: An industrial experience report. 2014 Software Evolution Week - IEEE Conference on Software Maintenance, Reengineering, and Reverse Engineering, CSMR-WCRE 2014 - Proceedings, 2014.	Göteborg
Araldo A., Dán G., Rossi D. Stochastic dynamic cache partitioning for encrypted content delivery. Proceedings of the 28th International Teletraffic Congress, ITC 2016, Vol. 1, 2017.	KTH
Argyriou M., Dragoni N., Spognardi A. Security flows in OAuth 2.0 framework: A case study. Lecture Notes in Computer Science (including	Örebro

subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10489 LNCS, 2017.	
Argyropoulos S., List P., Garcia M.-N., Feiten B., Pettersson M., Raake A. Scene change detection in encrypted video bit streams. 2013 IEEE International Conference on Image Processing, ICIP 2013 - Proceedings, 2013.	Ericsson
Armengol E., Torra V. Generalization-based k-anonymization. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9321, 2015.	Skövde
Armengol E., Torra V. Partial domain theories for privacy. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9880 LNAI, 2016.	Skövde
Arvidsson M., Sjöstrand J., Stage J. The economics of the Swedish online gambling market. Applied Economics Letters, vol. 24:16, 2017.	Luleå
Asadollah S.A., Sundmark D., Hansson H. Runtime Verification for Detecting Suspension Bugs in Multicore and Parallel Software. Proceedings - 10th IEEE International Conference on Software Testing, Verification and Validation Workshops, ICSTW 2017, 2017.	Mälardalen
Asghar M.R., Dán G., Miorandi D., Chlamtac I. Smart meter data privacy: A survey. IEEE Communications Surveys and Tutorials, vol. 19:4, 2017.	KTH
Ashcroft M., Kaati L., Meyer M. A Step Towards Detecting Online Grooming-Identifying Adults Pretending to be Children. Proceedings - 2015 European Intelligence and Security Informatics Conference, EISIC 2015, 2016.	Uppsala
Aslam M., Gehrmann C., Björkman M. Continuous security evaluation and auditing of remote platforms by combining trusted computing and security automation techniques. SIN 2013 - Proceedings of the 6th International Conference on Security of Information and Networks, 2013.	Mälardalen, SICS
Athanasopoulos E., Boehner M., Giuffrida C., Pidan D., Prevelakis V., Sourdis I., Strydis C., Thomson J. Increasing the trustworthiness of embedded applications. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9229, 2015.	Chalmers
Athanasopoulos E., Boehner M., Ioannidis S., Giuffrida C., Pidan D., Prevelakis V., Sourdis I., Strydis C., Thomson J. Secure hardware-software architectures for robust computing systems. Communications in Computer and Information Science, Vol. 570, 2015.	Chalmers

Austrin P., Chung K.-M., Mahmoody M., Pass R., Seth K. On the Impossibility of Cryptography with Tamperable Randomness. Algorithmica, vol. 79:4, 2017.	KTH
Austrin P., Chung K.-M., Mahmoody M., Pass R., Seth K. On the impossibility of cryptography with tamperable randomness. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 8616 LNCS:PART 1, 2014.	KTH
Austrin P., Kaski P., Koivisto M., Määttä J. Space-time tradeoffs for subset sum: An improved worst case algorithm. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 7965 LNCS:PART 1, 2013.	KTH
Awad A.I. Fast fingerprint orientation field estimation incorporating general purpose GPU. Advances in Intelligent Systems and Computing, Vol. 357, 2016.	Luleå
Awad A.I. Fingerprint local invariant feature extraction on GPU with CUDA. Informatica (Slovenia), vol. 37:3, 2013.	Luleå
Awad A.I. From classical methods to animal biometrics: A review on cattle identification and tracking. Computers and Electronics in Agriculture, Vol. 123, 2016.	Luleå
Ayalew T., Kidane T., Carlsson B. Identification and evaluation of security activities in agile projects. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8208 LNCS, 2013.	Blekinge
Babaheidarian P., Salimi S., Papadimitratos P. Preserving confidentiality in the Gaussian broadcast channel using compute-and-forward. 2017 51st Annual Conference on Information Sciences and Systems, CISS 2017, 2017.	KTH
Baca D., Boldt M., Carlsson B., Jacobsson A. A novel security-enhanced agile software development process applied in an industrial setting. Proceedings - 10th International Conference on Availability, Reliability and Security, ARES 2015, 2015.	Blekinge, Ericsson, Malmö
Baca D., Carlsson B., Petersen K., Lundberg L. Improving software security with static automated code analysis in an industry setting. Software - Practice and Experience, vol. 43:3, 2013.	Blekinge
Baca D., Petersen K. Countermeasure graphs for software security risk assessment: An action research. Journal of Systems and Software, vol. 86:9, 2013.	Blekinge
Bagci I.E., Raza S., Chung T., Roedig U., Voigt T. Combined secure storage and communication for the Internet of Things. 2013 IEEE	SICS, Uppsala

International Conference on Sensing, Communications and Networking, SECON 2013, 2013.	
Bagci I.E., Raza S., Roedig U., Voigt T. Fusion: coalesced confidential storage and communication framework for the IoT. Security and Communication Networks, vol. 9:15, 2016.	SICS, Uppsala
Bahri L. Identity related threats, vulnerabilities and risk mitigation in online social networks: A tutorial. Proceedings of the ACM Conference on Computer and Communications Security, Vol. Part F131467, 2017.	KTH
Balliu M., Dam M., Guanciale R. Automating information flow analysis of low level code. Proceedings of the ACM Conference on Computer and Communications Security, 2014.	KTH
Balozian P., Leidner D. Review of IS security policy compliance: Toward the building blocks of an IS asecurity theory. Data Base for Advances in Information Systems, vol. 48:3, 2017.	Lund
Barros B.M., Iwaya L.H., Simplicio M.A., Jr., Carvalho T.C.M.B., Méhes A., Näslund M. Classifying security threats in cloud networking. CLOSER 2015 - 5th International Conference on Cloud Computing and Services Science, Proceedings, 2015.	Ericsson, Karlstad
Batalla J.M., Vasilakos A., Gajewski M. Secure Smart Homes: Opportunities and challenges. ACM Computing Surveys, vol. 50:5, 2017.	Luleå
Baumann C., Naslund M., Gehrmann C., Schwarz O., Thorsen H. A high assurance virtualization platform for ARMv8. EUCNC 2016 - European Conference on Networks and Communications, 2016.	Ericsson, KTH, SICS
Beckman L., Hagquist C., Hellström L. Discrepant gender patterns for cyberbullyiyng and traditional bullying - An analysis of Swedish adolescent data. Computers in Human Behavior, vol. 29:5, 2013.	Karlstad
Beckman L., Rosenberg J.H. Freedom as Non-domination and Democratic Inclusion. Res Publica, 2017.	Stockholm
Behrensen M. Identity as convention: Biometric passports and the promise of security. Journal of Information, Communication and Ethics in Society, vol. 12:1, 2014.	Linköping
Bella G., Giustolisi R., Lenzini G., Ryan P.Y.A. Trustworthy exams without trusted parties. Computers and Security, Vol. 67, 2017.	SICS
Bello L., Hedin D., Sabelfeld A. Value sensitivity and observable abstract values for information flow control. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9450, 2015.	Chalmers
Ben Dhaou I., Gia T.N., Liljeberg P., Tenhunen H. Low-latency hardware architecture for cipher-based message authentication code.	KTH

Proceedings - IEEE International Symposium on Circuits and Systems, 2017.	
Ben Henda N., Johansson B., Lantz P., Norrman K., Saarinen P., Segersvärd O. OpenSAW: Open security analysis workbench. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10202 LNCS, 2017.	Ericsson, KTH
Ben Henda N., Norrman K. Formal analysis of security procedures in LTE - A feasibility study. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8688 LNCS, 2014.	Ericsson
Bera S., Misra S., Vasilakos A.V., Prof. Dr. Software-Defined Networking for Internet of Things: A Survey. IEEE Internet of Things Journal, vol. 4:6, 2017.	Luleå
Berger C., Block D., Heeren S., Hons C., Kühnel S., Leschke A., Plotnikov D., Rumpe B. Simulations on Consumer Tests: A Systematic Evaluation Approach in an Industrial Case Study. IEEE Intelligent Transportation Systems Magazine, vol. 7:4, 2015.	Göteborg
Bergström A. Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. Computers in Human Behavior, Vol. 53, 2015.	Göteborg
Bergström E., Åhlfeldt R.-M. Information classification issues. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8788, 2014.	Skövde
Bergström I., Blackwell A.F. The practices of programming. Proceedings of IEEE Symposium on Visual Languages and Human-Centric Computing, VL/HCC, Vol. 2016-November, 2016.	KTH
Berne S., Frisén A., Kling J. Appearance-related cyberbullying: A qualitative investigation of characteristics, content, reasons, and effects. Body Image, vol. 11:4, 2014.	Göteborg
Berntsson P.S., Strandén L., Warg F. Evaluation of open source operating systems for safety-critical applications. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10479 LNCS, 2017.	Chalmers
Bhatt P., Yano E.T., Amorim J., Gustavsson P. A cyber security situational awareness framework to track and project multistage cyber attacks. 9th International Conference on Cyber Warfare and Security 2014, ICCWS 2014, 2014.	Skövde
Bicaku A., Maksuti S., Palkovits-Rauter S., Tauber M., Matischek R., Schmittner C., Mantas G., Thron M., Delsing J. Towards trustworthy	Luleå

end-to-end communication in industry 4.0. Proceedings - 2017 IEEE 15th International Conference on Industrial Informatics, INDIN 2017, 2017.	
Björck F., Henkel M., Stirna J., Zdravkovic J. Cyber resilience – Fundamentals for a definition. Advances in Intelligent Systems and Computing, Vol. 353, 2015.	Stockholm
Blazquez A., Tsiatsis V., Vandikas K. Performance evaluation of OpenID connect for an IoT information marketplace. IEEE Vehicular Technology Conference, Vol. 2015, 2015.	Ericsson
Blom R., Korman M., Lagerstrom R., Ekstedt M. Analyzing attack resilience of an advanced meter infrastructure reference model. IEEE Proceedings of the 2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids, CPSR-SG 2016 - This Workshop is Part of the CPS Week 2016, 2016.	KTH
Bodriagov O., Kreitz G., Buchegger S. Access control in decentralized online social networks: Applying a policy-hiding cryptographic scheme and evaluating its performance. 2014 IEEE International Conference on Pervasive Computing and Communication Workshops, PERCOM WORKSHOPS 2014, 2014.	KTH
Bohli J.-M., Kurpatov R., Schmidt M. Selective decryption of outsourced IoT data. IEEE World Forum on Internet of Things, WF-IoT 2015 - Proceedings, 2015.	Luleå
Booth T., Andersson K. Critical infrastructure network DDoS defense, via cognitive learning. 2017 14th IEEE Annual Consumer Communications and Networking Conference, CCNC 2017, Vol. 2017-January, 2017.	Luleå
Booth T., Andersson K. DNS DDoS mitigation, via DNS timer design changes. Communications in Computer and Information Science, Vol. 759, 2017.	Luleå
Booth T., Andersson K. Network DDoS layer 3/4/7 mitigation via dynamic web redirection. Communications in Computer and Information Science, Vol. 670, 2016.	Luleå
Booth T., Andersson K. Stronger authentication for password credential Internet Services. Proceedings of the 2017 3rd Conference on Mobile and Secure Services, MOBISECSERV 2017, 2017.	Luleå
Booth T.G., Andersson K. Elimination of DoS UDP reflection amplification bandwidth attacks, protecting TCP services. Communications in Computer and Information Science, Vol. 523, 2015.	Luleå
Borg M., Wnuk K., Regnell B., Runeson P. Supporting Change Impact Analysis Using a Recommendation System: An Industrial Case Study in a Safety-Critical Context. IEEE Transactions on Software Engineering, vol. 43:7, 2017.	Blekinge

Borges F., Martucci L.A. IKUP keeps users' privacy in the Smart Grid. 2014 IEEE Conference on Communications and Network Security, CNS 2014, 2014.	Karlstad
Borges F., Martucci L.A., Beato F., Muhlhauser M. Secure and privacy-friendly public key generation and certification. Proceedings - 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2014, 2015.	Karlstad
Borgh J., Ngai E., Ohlman B., Malik A.M. Employing attribute-based encryption in systems with resource constrained devices in an information-centric networking context. GIoTS 2017 - Global Internet of Things Summit, Proceedings, 2017.	Ericsson, Uppsala
Borgström J., Gutkovas R., Parrow J., Victor B., Pohjola J.Å. A sorted semantic framework for applied process calculi. Logical Methods in Computer Science, vol. 12:1, 2016.	Uppsala
Borisenko K., Rukavitsyn A., Gurtov A., Shorov A. Detecting the origin of DDoS attacks in OpenStack cloud platform using data mining techniques. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9870 LNCS, 2016.	Linköping
Bosk D., Buchegger S. Privacy-preserving access control in publicly readable storage systems. IFIP Advances in Information and Communication Technology, Vol. 476, 2016.	KTH
Bosk D., Kjellqvist M., Buchegger S. Towards perfectly secure and deniable communication using an NFC-based key-exchange scheme. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9417, 2015.	KTH, Mitt
Breivold H.P., Crnkovic I., Radosevic I., Balatinac I. Architecting for the cloud: A systematic review. Proceedings - 17th IEEE International Conference on Computational Science and Engineering, CSE 2014, Jointly with 13th IEEE International Conference on Ubiquitous Computing and Communications, IUCC 2014, 13th International Symposium on Pervasive Systems, Algorithms, and Networks, I-SPAN 2014 and 8th International Conference on Frontier of Computer Science and Technology, FCST 2014, 2015.	ABB
Broberg N., Van Delft B., Sands D. Paragon for practical programming with information-flow control. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8301 LNCS, 2013.	Chalmers
Brodin M. Combining isms with strategic management: The case of BYOD. Proceedings of the 8th IADIS International Conference Information Systems 2015, IS 2015, 2015.	Skövde

Brunetta C., Dimitrakakis C., Liang B., Mitrokotsa A. A Differentially Private Encryption Scheme. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10599 LNCS, 2017.	Chalmers
Brynielsson J., Franke U., Adnan Tariq M., Varga S. Using cyber defense exercises to obtain additional data for attacker profiling. IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data, ISI 2016, 2016.	FOI, KTH, SICS
Brynielsson J., Sharma R. Detectability of low-rate HTTP server DoS attacks using spectral analysis. Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2015, 2015.	FOI, KTH
Buckholtz B., Ragai I., Wang L. Remote equipment security in cloud manufacturing systems. International Journal of Manufacturing Research, vol. 11:2, 2016.	KTH
Bugeja J., Jacobsson A., Davidsson P. An analysis of malicious threat agents for the smart connected home. 2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017, 2017.	Malmö
Bugeja J., Jacobsson A., Davidsson P. On privacy and security challenges in smart connected homes. Proceedings - 2016 European Intelligence and Security Informatics Conference, EISIC 2016, 2017.	Malmö
Buiras P., Russo A. Lazy programs leak secrets. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8208 LNCS, 2013.	Chalmers
Burden H., Heldal R., Ljunglöf P. Enabling interface validation through text generation. 5th International Conference on Advances in System Testing and Validation Lifecycle, VALID 2013, Held at SoftNet 2013, 2013.	Chalmers
Cajander A., Grünloh C., Lind T., Scandurra I. Designing ehealth services for patients and relatives: Critical incidents and lessons to learn. ACM International Conference Proceeding Series, Vol. 23-27-October-2016, 2016.	KTH
Callau-Zori M., Gulisano V., Fu Z., Jiménez-Peris R., Papatriantafilou M., Patiño-Martínez M. STONE: A stream-based DDoS defense framework. Proceedings of the ACM Symposium on Applied Computing, 2013.	Chalmers
Callele D., Penzenstadler B., Wnuk K. Risk identification at the interface between business case and requirements. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 7830 LNCS, 2013.	Lund

Caltais G., Leue S., Mousavi M.R. (De-)composing causality in labeled transition systems. Electronic Proceedings in Theoretical Computer Science, EPTCS, Vol. 224, 2016.	Halmstad
Cambazoglu V., Thota N. Computer science students' perception of computer network security. Proceedings - 2013 Learning and Teaching in Computing and Engineering, LaTiCE 2013, 2013.	Uppsala
Cao Z., Zhang S., Ji X., Zhang L. Secure random linear network coding on a wiretap network. AEU - International Journal of Electronics and Communications, vol. 69:1, 2014.	Umeå
Carlsson A. Model of network attack on the cloud platform OpenStack. 2015 2nd International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2015 - Conference Proceedings, 2015.	Blekinge
Carlsson M., Grinchtein O., Pearson J. Protocol log analysis with constraint programming (work in progress). CEUR Workshop Proceedings, Vol. 1163, 2014.	SICS
Carvalho J.M., Brãs S., Ferreira J., Soares S.C., Pinho A.J. Impact of the acquisition time on ECG compression-based biometric identification systems. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10255 LNCS, 2017.	Karolinska
Cassel S., Nylén A., Victor B. Enhanced learning by promoting engineering competencies. Proceedings - Frontiers in Education Conference, FIE, vol. 2015-February:February, 2015.	Uppsala
Ceccato M., Scandariato R. Static Analysis and Penetration Testing from the Perspective of Maintenance Teams. International Symposium on Empirical Software Engineering and Measurement, Vol. 08-09-September-2016, 2016.	Chalmers
Charif B., Awad A.I. Business and government organizations' adoption of cloud computing. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8669, 2014.	Luleå
Charif B., Awad A.I. Towards smooth organisational adoption of cloud computing - A customer-provider security adaptation. Computer Fraud and Security, vol. 2016:2, 2016.	Luleå
Chattopadhyay S., Beck M., Rezine A., Zeller A. Quantifying the information leak in cache atacks via symbolic execution. MEMOCODE 2017 - 15th ACM-IEEE International Conference on Formal Methods and Models for System Design, 2017.	Linköping
Chen D., Meinke K., Ostberg K., Asplund F., Baumann C. A knowledge-in-the-loop approach to integrated safety & security for cooperative	KTH

system-of-systems. 2015 IEEE 7th International Conference on Intelligent Computing and Information Systems, ICICIS 2015, 2016.	
Chen J., Liu Z., Mendoza P.A., Chen F. Acceptance of integrated active safety systems in China. Communications in Computer and Information Science, Vol. 529, 2015.	Chalmers
Chen J., Wei J., Chen W., Sandberg H., Johansson K.H., Chen J. Protecting Positive and Second-Order Systems against Undetectable Attacks. IFAC-PapersOnLine, vol. 50:1, 2017.	KTH
Cheng Q., Lu X., Liu Z., Huang J. Mining research trends with anomaly detection models: the case of social computing research. Scientometrics, vol. 103:2, 2015.	Karolinska
Chenine M., Ullberg J., Nordstrom L., Wu Y., Ericsson G.N. A framework for wide-area monitoring and control systems interoperability and cybersecurity analysis. IEEE Transactions on Power Delivery, vol. 29:2, 2014.	KTH
Cherkaoui A., Bossuet L., Seitz L., Selander G., Borgaonkar R. New paradigms for access control in constrained environments. 2014 9th International Symposium on Reconfigurable and Communication-Centric Systems-on-Chip, ReCoSoC 2014, 2014.	Ericsson
Chfouka H., Nemati H., Guanciale R., Dam M., Ekdahl P. Trustworthy prevention of code injection in Linux on embedded devices. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9326, 2015.	Ericsson, KTH
Chiaraviglio L., Wiatr P., Monti P., Chen J., Lorincz J., Idzikowski F., Listanti M., Wosinska L. Is green networking beneficial in terms of device lifetime?. IEEE Communications Magazine, vol. 53:5, 2015.	KTH
Chipidza W., Leidner D., Burleson D. Why companies change privacy policies: A principal-agent perspective. Proceedings of the Annual Hawaii International Conference on System Sciences, Vol. 2016-March, 2016.	Lund
Christin D., Roßkopf C., Hollick M., Martucci L.A., Kanhere S.S. IncogniSense: An anonymity-preserving reputation framework for participatory sensing applications. Pervasive and Mobile Computing, vol. 9:3, 2013.	Linköping
Chu T.M.C., Zepernick H.-J., Phan H. Optimal secrecy capacity of underlay cognitive radio networks with multiple relays. Proceedings - IEEE Military Communications Conference MILCOM, 2016.	Blekinge
Claessen K., Pałka M.H. Splittable pseudorandom number generators using cryptographic hashing. ACM SIGPLAN Notices, vol. 48:12, 2014.	Chalmers

Claessen K., Pałka M.H. Splittable pseudorandom number generators using cryptographic hashing. Proceedings of the ACM SIGPLAN International Conference on Functional Programming, ICFP, 2013.	Chalmers
Cohen K., Johansson F., Kaati L., Mork J.C. Detecting Linguistic Markers for Radical Violence in Social Media. Terrorism and Political Violence, vol. 26:1, 2014.	FOI
Colonese E., De Oliveira J.P., Yano E., Amorim J., Andler S., Gustavsson P. Cyber security for middleware system architectures. 9th International Conference on Cyber Warfare and Security 2014, ICCWS 2014, 2014.	FHS, Skövde
Conti M., Dragoni N., Lesyk V. A Survey of Man in the Middle Attacks. IEEE Communications Surveys and Tutorials, vol. 18:3, 2016.	Örebro
Cooper K., Quayle E., Jonsson L., Svedin C.G. Adolescents and self-taken sexual images: A review of the literature. Computers in Human Behavior, Vol. 55, 2016.	Linköping
Correia F., Mariano A., Proenca A., Bischof C., Agrell E. Parallel Improved Schnorr-Euchner Enumeration SE++ for the CVP and SVP. Proceedings - 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing, PDP 2016, 2016.	Chalmers
Croicu M., Kreutz J. Communication Technology and Reports on Political Violence: Cross-National Evidence Using African Events Data. Political Research Quarterly, vol. 70:1, 2017.	Uppsala
Da Silva J.M.B., Jr., Fodor G., Maciel T.F. Performance analysis of network-assisted two-hop D2D communications. 2014 IEEE Globecom Workshops, GC Wkshps 2014, 2014.	Ericsson
Dahlberg R., Pulls T., Peeters R. Efficient sparse merkle trees caching strategies and secure (Non-) Membership proofs. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10014 LNCS, 2016.	Karlstad
Dam M., Jacobs B., Lundblad A., Piessens F. Security monitor inlining and certification for multithreaded Java. Mathematical Structures in Computer Science, vol. 25:3, 2015.	KTH
Dán G., Lui K.-S., Tabassum R., Zhu Q., Nahrstedt K. SELINDA: A secure, scalable and light-weight data collection protocol for smart grids. 2013 IEEE International Conference on Smart Grid Communications, SmartGridComm 2013, 2013.	KTH
Darwaish S.F., Moradian E., Rahmani T., Knauer M. Biometric identification on android smartphones. Procedia Computer Science, vol. 35:C, 2014.	Stockholm

Davidson A., de La Puente Martinez J., Huber M. A SWOT analysis of virtual laboratories for security education. IFIP Advances in Information and Communication Technology, Vol. 406, 2013.	KTH, Stockholm
De Carvalho Gomes P., Gurov D., Huisman M. Specification and verification of synchronization with condition variables. Communications in Computer and Information Science, Vol. 694, 2017.	KTH
De Donno M., Dragoni N., Giaretta A., Mazzara M. AntibIoTic: Protecting IoT devices against DDoS attacks. Advances in Intelligent Systems and Computing, Vol. 717, 2018.	Örebro
De Donno M., Dragoni N., Giaretta A., Spognardi A. Analysis of DDoS-capable IoT malwares. Proceedings of the 2017 Federated Conference on Computer Science and Information Systems, FedCSIS 2017, 2017.	Örebro
De Donno M., Dragoni N., Giaretta A., Spognardi A. DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation. Security and Communication Networks, Vol. 2018, 2018.	Örebro
Del Tedesco F., Russo A., Sands D. Fault-tolerant non-interference. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8364 LNCS, 2014.	Chalmers
Demesie Yalew S., Maguire G.Q., Haridi S., Correia M. DroidPosture: A trusted posture assessment service for mobile devices. International Conference on Wireless and Mobile Computing, Networking and Communications, Vol. 2017-October, 2017.	KTH
Demesie Yalew S., Mendonca P., Maguire G.Q., Haridi S., Correia M. TruApp: A TrustZone-based authenticity detection service for mobile apps. International Conference on Wireless and Mobile Computing, Networking and Communications, Vol. 2017-October, 2017.	KTH
Deng R., Xiao G., Lu R., Liang H., Vasilakos A.V. False data injection on state estimation in power systems-attacks, impacts, and defense: A survey. IEEE Transactions on Industrial Informatics, vol. 13:2, 2017.	Luleå
Derhamy H., Eliasson J., Delsing J., Priller P. A survey of commercial frameworks for the Internet of Things. IEEE International Conference on Emerging Technologies and Factory Automation, ETFA, Vol. 2015-October, 2015.	Luleå
Dhaou I.B., Kondoro A., Kelati A., Rwegasira D.S., Naiman S., Mvungi N.H., Tenhunen H. Communication and security technologies for smart grid. International Journal of Embedded and Real-Time Communication Systems, vol. 8:2, 2017.	KTH
Dhillon G., Harnesk D. Misunderstandings and misjudgments about security: A dialogical narrative analysis of global it offshoring. AMCIS	Luleå

2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems, 2016.	
Di Mauro A., Fafoutis X., Dragoni N. Adaptive security in ODMAC for multihop energy harvesting wireless sensor networks. International Journal of Distributed Sensor Networks, Vol. 2015, 2015.	Örebro
Dimitrakakis C., Mitrokotsa A. Distance-Bounding Protocols: Are You Close Enough?. IEEE Security and Privacy, vol. 13:4, 2015.	Chalmers
Dimitrakakis C., Mitrokotsa A. Near-optimal blacklisting. Computers and Security, Vol. 64, 2017.	Chalmers
Ding J., Atif Y., Andler S.F., Lindström B., Jeusfeld M. CPS-based threat modeling for critical infrastructure protection. Performance Evaluation Review, vol. 45:2, 2017.	Skövde
Ding K., Li Y., Quevedo D.E., Dey S., Shi L. A multi-channel transmission schedule for remote state estimation under DoS attacks. Automatica, Vol. 78, 2017.	Uppsala
Ding K., Quevedo D.E., Dey S., Shi L. A secure cross-layer design for remote estimation under DoS attack: When multi-sensor meets multi-channel. 2016 IEEE 55th Conference on Decision and Control, CDC 2016, 2016.	Uppsala
Dini G., Tiloca M. A simulation tool for evaluating attack impact in cyber physical systems. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8906, 2014.	SICS
Dolev S., Georgiou C., Marcoullis I., Schiller E.M. Self-stabilizing virtual synchrony. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9212, 2015.	Chalmers
Dolev S., Liba O., Schiller E.M. Self-stabilizing Byzantine resilient topology discovery and message delivery (Extended abstract). Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 7853 LNCS, 2013.	Chalmers
Dolev S., Panagopoulou P.N., Rabie M., Schiller E.M., Spirakis P.G. Rationality authority for provable rational behavior. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9295, 2015.	Chalmers
Dolev S., Petig T., Schiller E.M. Brief announcement: Robust and private distributed shared atomic memory in message passing networks. Proceedings of the Annual ACM Symposium on Principles of Distributed Computing, Vol. 2015-July, 2015.	Chalmers

Domova V., Dagnino A. Towards intelligent alarm management in the Age of IIoT. GIoTS 2017 - Global Internet of Things Summit, Proceedings, 2017.	ABB
Dosis S., Homem I., Popov O. Semantic representation and integration of digital evidence. Procedia Computer Science, Vol. 22, 2013.	Stockholm
Dowsley R., Michalas A., Nagel M., Paladi N. A survey on design and implementation of protected searchable data in the cloud. Computer Science Review, Vol. 26, 2017.	SICS
Dragoni N., Giaretta A., Mazzara M. The internet of hackable things. Advances in Intelligent Systems and Computing, Vol. 717, 2018.	Örebro
Duan J., Yang D., Zhang S., Zhao J., Gidlund M. A trust management scheme for industrial wireless sensor networks. IECON Proceedings (Industrial Electronics Conference), 2013.	ABB
Dubrova E., Hell M. Espresso: A stream cipher for 5G wireless communication systems. Cryptography and Communications, vol. 9:2, 2017.	KTH, Lund
Dubrova E., Naslund M., Carlsson G., Smeets B. Keyed logic BIST for Trojan detection in SoC. 2014 International Symposium on System-on-Chip, SoC 2014, 2014.	Ericsson, KTH
Dubrova E., Näslund M., Carlsson G., Fornehed J., Smeets B. Two Countermeasures Against Hardware Trojans Exploiting Non-Zero Aliasing Probability of BIST. Journal of Signal Processing Systems, vol. 87:3, 2017.	Ericsson, KTH
Dubrova E., Näslund M., Selander G. CRC-based message authentication for 5G mobile technology. Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015, Vol. 1, 2015.	Ericsson, KTH
Dubrova E., Näslund M., Selander G. Secure and efficient LBIST for feedback shift register-based cryptographic systems. Proceedings - 2014 19th IEEE European Test Symposium, ETS 2014, 2014.	Ericsson, KTH
Dubrova E., Näslund M., Selander G., Lindqvist F. Message Authentication Based on Cryptographically Secure CRC without Polynomial Irreducibility Test. Cryptography and Communications, vol. 10:2, 2018.	Ericsson, KTH
Duc A.N., Jabangwe R., Paul P., Abrahamsson P. Security challenges in IoT development: A software engineering perspective. ACM International Conference Proceeding Series, Vol. Part F129907, 2017.	Blekinge
Duracz A., Eriksson H., Bartha F.A., Xu F., Zeng Y., Taha W. Using rigorous simulation to support ISO 26262 hazard analysis and risk assessment. Proceedings - 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th	Halmstad

International Symposium on Cyberspace Safety and Security and 2015 IEEE 12th International Conference on Embedded Software and Systems, HPCC-CSS-ICESS 2015, 2015.	
Ebadi H., Sands D., Schneider G. Differential privacy: Now it's getting personal. Conference Record of the Annual ACM Symposium on Principles of Programming Languages, Vol. 2015-January, 2015.	Chalmers, Göteborg
Ehatisham-Ul-Haq M., Azam M.A., Naeem U., Rehman S.U., Khalid A. Identifying Smartphone Users based on their Activity Patterns via Mobile Sensing. Procedia Computer Science, Vol. 113, 2017.	Umeå
Ehdaie M., Alexiou N., Ahmadian M., Aref M.R., Papadimitratos P. 2D Hash Chain robust Random Key Distribution scheme. Information Processing Letters, vol. 116:5, 2016.	KTH
Ehdaie M., Alexiou N., Attari M.A., Aref M.R., Papadimitratos P. Key splitting: Making random key distribution schemes resistant against node capture. Security and Communication Networks, vol. 8:3, 2015.	KTH
Ekerå M., Håstad J. Quantum algorithms for computing short discrete logarithms and factoring RSA integers. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10346 LNCS, 2017.	KTH
Ekman F., Johansson M., Sochor J. Creating appropriate trust in automated vehicle systems: A framework for HMI design. IEEE Transactions on Human-Machine Systems, vol. 48:1, 2018.	Chalmers
Ekman F., Johansson M., Sochor J. To see or not to see-the effect of object recognition on users' Trust in "automated Vehicles". ACM International Conference Proceeding Series, Vol. 23-27-October-2016, 2016.	Chalmers
Ekstedt M., Johnson P., Lagerström R., Gorton D., Nydrén J., Shahzad K. SecuriCAD by foreseeti: A CAD tool for enterprise cyber security management. Proceedings of the 2015 IEEE 19th International Enterprise Distributed Object Computing Conference Workshops and Demonstrations, EDOCW 2015, 2015.	KTH
El Mekawy M., AlSabbagh B., Kowalski S. The impact of business-IT alignment on information security process. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8527 LNCS, 2014.	Stockholm
Elmisery A.M., Rho S., Botvich D. Privacy-enhanced middleware for location-based sub-community discovery in implicit social groups. Journal of Supercomputing, vol. 72:1, 2016.	Malmö
Elowsson A., Friberg A. Long-term average spectrum in popular music and its rela-tion to the level of the percussion. 142nd Audio Engineering Society International Convention 2017, AES 2017, 2017.	KTH

Elrawy M.F., Awad A.I., Hamed H.F.A. Flow-based features for a robust intrusion detection system targeting mobile traffic. 2016 23rd International Conference on Telecommunications, ICT 2016, 2016.	Luleå
Eriksson A., Kjellström H. A formal approach to anomaly detection. ICPRAM 2016 - Proceedings of the 5th International Conference on Pattern Recognition Applications and Methods, 2016.	KTH
Eriksson E., Artman H., Swartling A. The secret life of a persona: When the personal becomes private. Conference on Human Factors in Computing Systems - Proceedings, 2013.	KTH
Eriksson G.A.P., Mattsson J., Mitra N., Sarker Z. Blind cache: A solution to content delivery challenges in an all-encrypted web. Ericsson Review (English Edition), vol. 94:1, 2017.	KTH, Luleå, Stockholm
Ersson J., Moradian E. Botnet detection with event-driven analysis. Procedia Computer Science, Vol. 22, 2013.	Stockholm
Fabšič T., Hromada V., Stankovski P., Zajac P., Guo Q., Johansson T. A reaction attack on the QC-LDPC mceliece cryptosystem. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10346 LNCS, 2017.	Lund
Famurewa S.M., Zhang L., Asplund M. Maintenance analytics for railway infrastructure decision support. Journal of Quality in Maintenance Engineering, vol. 23:3, 2017.	Luleå
Farokhi F., Shames I., Rabbat M.G., Johansson M. On reconstructability of quadratic utility functions from the iterations in gradient methods. Automatica, Vol. 66, 2016.	KTH
Fernandez-Gago C., Pearson S., D'Errico M., Alnemr R., Pulls T., de Oliveira A.S. A4Cloud workshop: Accountability in the cloud. IFIP Advances in Information and Communication Technology, Vol. 476, 2016.	Karlstad
Fernández-Sáez A.M., Chaudron M.R.V., Genero M., Ramos I. Are forward designed or reverse-engineered UML diagrams more helpful for code maintenance?: A controlled experiment. ACM International Conference Proceeding Series, 2013.	Chalmers
Ferreira P., Sanches P., Weilenmann A. Awareness, transience and temporality: Design opportunities from Rah Island. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 8118 LNCS:PART 2, 2013.	KTH
Figea L., Kaati L., Scrivens R. Measuring online affects in a white supremacy forum. IEEE International Conference on Intelligence and Security Informatics: Cybersecurity and Big Data, ISI 2016, 2016.	Uppsala

Fiore D., Mitrokotsa A., Nizzardo L., Pagnin E. Multi-key homomorphic authenticators. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10032 LNCS, 2016.	Chalmers
Fischer-Hübner S., Angulo J., Karegar F., Pulls T. Transparency, privacy and trust – Technology for tracking and controlling my data disclosures: Does this work?. IFIP Advances in Information and Communication Technology, Vol. 473, 2016.	Karlstad
Fischer-Hübner S., Angulo J., Pulls T. How can cloud users be supported in deciding on, tracking and controlling how their data are used?. IFIP Advances in Information and Communication Technology, Vol. 421, 2014.	Karlstad
Fischer-Hübner S., Pettersson J.S., Angulo J. HCI requirements for transparency and accountability tools for cloud service chains. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8937, 2015.	Karlstad
Flores W., Ekstedt M. Exploring the link between behavioural information security governance and employee information security awareness. Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015, 2015.	KTH
Flores W.R. Establishment of security knowledge sharing in organisations: An empirical study. Proceedings of the European Information Security Multi-Conference, EISMC 2013, 2013.	KTH
Flores W.R., Holm H., Ekstedt M., Nohlberg M. Investigating the correlation between intention and action in the context of social engineering in two different national cultures. Proceedings of the Annual Hawaii International Conference on System Sciences, Vol. 2015-March, 2015.	FOI, KTH, Skövde
Flores W.R., Holm H., Nohlberg M., Ekstedt M. Investigating personal determinants of phishing and the effect of national culture. Information and Computer Security, vol. 23:2, 2015.	FOI, KTH, Skövde
Flores W.R., Holm H., Svensson Gu., Ericsson G. Using phishing experiments and scenario-based surveys to understand security behaviours in practice. Proceedings of the European Information Security Multi-Conference, EISMC 2013, 2013.	KTH
Forssell R. Exploring cyberbullying and face-to-face bullying in working life - Prevalence, targets and expressions. Computers in Human Behavior, Vol. 58, 2016.	Malmö
Fragkiadakis A., Angelakis V., Tragos E.Z. Securing cognitive wireless sensor networks: A survey. International Journal of Distributed Sensor Networks, Vol. 2014, 2014.	Linköping

Franke U. The cyber insurance market in Sweden. Computers and Security, Vol. 68, 2017.	SICS
Franke U., Brynielsson J. Cyber situational awareness - A systematic review of the literature. Computers and Security, Vol. 46, 2014.	FOI
Franke U., Holm H., König J. The distribution of time to recovery of enterprise IT services. IEEE Transactions on Reliability, vol. 63:4, 2014.	FOI, KTH
Franke U., Rosell M. Prospects for detecting deception on twitter. Proceedings - 2014 International Conference on Future Internet of Things and Cloud, FiCloud 2014, 2014.	FOI
Fritsch L. Partial commitment-“Try before you buy” and “Buyer’s remorse” for personal data in big data & machine learning. IFIP Advances in Information and Communication Technology, Vol. 505, 2017.	Karlstad
Furdek M., Wosinska L., Goscien R., Manousakis K., Aibin M., Walkowiak K., Ristov S., Gushev M., Marzo J.L. An overview of security challenges in communication networks. Proceedings of 2016 8th International Workshop on Resilient Networks Design and Modeling, RNDM 2016, 2016.	KTH
Futcher L., Yngström L. A review of IFIP TC 11 WG 11.8 publications through the ages. IFIP Advances in Information and Communication Technology, Vol. 406, 2013.	KTH, Stockholm
Gabrielsson B., Fors K., Eliardsson P., Alexandersson M., Stenumgaard P. A portable system for autonomous detection and classification of electromagnetic interference in the GPS band. IEEE International Symposium on Electromagnetic Compatibility, 2014.	FOI
Gamalielsson J., Jakobsson F., Lundell B., Feist J., Gustavsson T., Landqvist F. On the availability and effectiveness of open source software for digital signing of PDF documents. IFIP Advances in Information and Communication Technology, Vol. 451, 2015.	Skövde
Gandini E., Svedin J., Bryllert T., Llombart N. Optomechanical System Design for Dual-Mode Stand-Off Submillimeter Wavelength Imagers. IEEE Transactions on Terahertz Science and Technology, vol. 7:4, 2017.	Chalmers, FOI
Gangwar A., Joshi A., Singh A., Alonso-Fernandez F., Bigun J. IrisSeg: A fast and robust iris segmentation framework for non-ideal iris images. 2016 International Conference on Biometrics, ICB 2016, 2016.	Halmstad
Gehrke O., Heussen K., Korman M. Integrated multi-domain risk assessment using automated hypothesis testing. Proceedings - 2017 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, CPSR-SG 2017 (part of CPS Week), 2017.	KTH
Gehrmann C., Tiloca M., Hoglund R. SMACK: Short message authentication check against battery exhaustion in the Internet of	SICS

Things. 2015 12th Annual IEEE International Conference on Sensing, Communication, and Networking, SECON 2015, 2015.	
Geneiatakis D., Fovino I.N., Kounelis I., Stirparo P. A Permission verification approach for android mobile applications. Computers and Security, Vol. 49, 2015.	KTH
Geneiatakis D., Kounelis I., Loeschner J., Fovino I.N., Stirparo P. Security and Privacy in Mobile Cloud Under a Citizen's Perspective. Communications in Computer and Information Science, Vol. 182 CCIS, 2013.	KTH
Gerami M., Xiao M., Salimi S., Skoglund M. Secure partial repair in wireless caching networks with broadcast channels. 2015 IEEE Conference on Communications and NetworkSecurity, CNS 2015, 2015.	KTH
Gerami M., Xiao M., Salimi S., Skoglund M., Papadimitratos P. Optimal secure partial-repair in distributed storage systems. 2017 51st Annual Conference on Information Sciences and Systems, CISS 2017, 2017.	KTH, Uppsala
Gerber N., McDermott R., Volkamer M., Vogt J. Understanding information security compliance-why goal setting and rewards might be a bad idea. Proceedings of the 10th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2016, 2016.	Uppsala
Ghazawneh A., Henfridsson O. Balancing platform control and external contribution in third-party development: The boundary resources model. Information Systems Journal, vol. 23:2, 2013.	Chalmers
Ghiglieri M., Volkamer M., Renaud K. Exploring consumers' attitudes of smart TV related privacy risks. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10292 LNCS, 2017.	Karlstad
Gholami A., Dowling J., Laure E. A security framework for population-scale genomics analysis. Proceedings of the 2015 International Conference on High Performance Computing and Simulation, HPCS 2015, 2015.	KTH
Gholami A., Lind A.-S., Reichel J., Litton J.-E., Edlund A., Laure E. Privacy threat modeling for emerging biobankclouds. Procedia Computer Science, Vol. 37, 2014.	Karolinska, KTH, Uppsala
Gholami M.R., Gezici S., Ström E.G. TW-TOA based positioning in the presence of clock imperfections. Digital Signal Processing: A Review Journal, Vol. 59, 2016.	Chalmers
Giannetsos T., Dimitriou T. LDAC: A localized and decentralized algorithm for efficiently countering wormholes in mobile wireless networks. Journal of Computer and System Sciences, vol. 80:3, 2014.	KTH

Giannetsos T., Dimitriou T. Spy-sense: Spyware tool for executing stealthy exploits against sensor networks. HotWiSec 2013 - Proceedings of the 2013 ACM Workshop on Hot Topics on Wireless Network Security and Privacy, 2013.	KTH
Gisdakis S., Giannetsos T., Papadimitratos P. SHIELD: A data verification framework for participatory sensing systems. Proceedings of the 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2015, 2015.	KTH
Gisdakis S., Giannetsos T., Papadimitratos P. SPPEAR: Security & privacy-preserving architecture for participatory-sensing applications. WiSec 2014 - Proceedings of the 7th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2014.	KTH
Gisdakis S., Katselis D., Papadimitratos P. Allocating adversarial resources in wireless networks. European Signal Processing Conference, 2013.	KTH
Gisdakis S., Laganà M., Giannetsos T., Papadimitratos P. SEROSA: SERvice oriented security architecture for Vehicular Communications. IEEE Vehicular Networking Conference, VNC, 2013.	KTH
Gisdakis S., Manolopoulos V., Tao S., Rusu A., Papadimitratos P. Secure and privacy-preserving smartphone-based traffic information systems. IEEE Transactions on Intelligent Transportation Systems, vol. 16:3, 2015.	KTH
Giustolisi R., Gehrmann C. Threats to 5G group-based authentication. ICETE 2016 - Proceedings of the 13th International Joint Conference on e-Business and Telecommunications, Vol. 4, 2016.	SICS
Giustolisi R., Gehrmann C., Ahlström M., Holmberg S. A secure group-based AKA protocol for machine-type communications. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10157 LNCS, 2017.	SICS
Giustolisi R., Iovino V., Rønne P.B. On the possibility of non-interactive e-voting in the public-key setting. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9604 LNCS, 2016.	SICS
Gordon T.J., Lidberg M. Automated driving and autonomous functions on road vehicles. Vehicle System Dynamics, vol. 53:7, 2015.	Chalmers
Gorton D. IncidentResponseSim: An agent-based simulation tool for risk management of online Fraud. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9417, 2015.	KTH

Goyal R., Dragoni N. Why hackers love ehealth applications. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, Vol. 187, 2016.	Örebro
Granger R., Moss A. Generalised mersenne numbers revisited. Mathematics of Computation, vol. 82:284, 2013.	Blekinge
Granlund D., Åhlund C., Holmlund P. EAP-swift: An efficient authentication and key generation mechanism for resource constrained WSNs. International Journal of Distributed Sensor Networks, Vol. 2015, 2015.	Luleå
Granåsen M., Andersson D. Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study. Cognition, Technology and Work, vol. 18:1, 2016.	FOI
Graydon P.J. Formal Assurance Arguments: A Solution in Search of a Problem?. Proceedings of the International Conference on Dependable Systems and Networks, Vol. 2015-September, 2015.	Mälardalen
Graydon P.J., Kelly T.P. Using argumentation to evaluate software assurance standards. Information and Software Technology, vol. 55:9, 2013.	Mälardalen
Grünloh C., Hallewell Haslwanter J.D., Kane B., Lee E., Lind T., Moll J., Rexhepi H., Scandurra I. Using critical incidents in workshops to inform eHealth design. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10513 LNCS, 2017.	KTH
Grzenda M., Furtak J., Legierski J., Awad A.I. Network architectures, security, and applications: An introduction. Advances in Intelligent Systems and Computing, Vol. 461, 2017.	Luleå
Guanciale R., Gurov D., Laud P. Private intersection of regular languages. 2014 12th Annual Conference on Privacy, Security and Trust, PST 2014, 2014.	KTH
Guanciale R., Nemati H., Baumann C., Dam M. Cache Storage Channels: Alias-Driven Attacks and Verified Countermeasures. Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016, 2016.	KTH
Guanciale R., Nemati H., Dam M., Baumann C. Provably secure memory isolation for Linux on ARM: Submission to special issue on Verified Information Flow Security. Journal of Computer Security, vol. 24:6, 2016.	KTH
Gulisano V., Almgren M., Papatriantafilou M. METIS: A two-tier intrusion detection system for advanced metering infrastructures. e-Energy 2014 - Proceedings of the 5th ACM International Conference on Future Energy Systems, 2014.	Chalmers

Gulisano V., Almgren M., Papatriantafilou M. METIS: A two-tier intrusion detection system for advanced metering infrastructures. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, Vol. 153, 2015.	Chalmers
Gulisano V., Callau-Zori M., Fu Z., Jiménez-Peris R., Papatriantafilou M., Patiño-Martínez M. STONE: A streaming DDoS defense framework. Expert Systems with Applications, vol. 42:24, 2015.	Chalmers
Gunneriusson H., Ottis R. Cyberspace from the hybrid threat perspective. European Conference on Information Warfare and Security, ECCWS, 2013.	FHS
Guo Q., Johansson T. A p-ary MDPC scheme. IEEE International Symposium on Information Theory - Proceedings, Vol. 2016-August, 2016.	Lund
Guo Q., Johansson T., Löndahl C. A New Algorithm for Solving Ring-LPN With a Reducible Polynomial. IEEE Transactions on Information Theory, vol. 61:11, 2015.	Lund
Guo Q., Johansson T., Löndahl C. Solving LPN using covering codes. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8873, 2014.	Lund
Guo Q., Johansson T., Martensson E., Stankovski P. Information set decoding with soft information and some cryptographic applications. IEEE International Symposium on Information Theory - Proceedings, 2017.	Lund
Guo Q., Johansson T., Mårtensson E., Stankovski P. Coded-BKW with sieving. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10624 LNCS, 2017.	Lund
Guo Q., Johansson T., Stankovski P. A key recovery attack on MDPC with CCA security using decoding errors. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10031 LNCS, 2016.	Lund
Guo Q., Johansson T., Stankovski P. Coded-BKW: Solving LWE using lattice codes. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9215, 2015.	Lund
Guo X., Leong A.S., Dey S. Estimation in Wireless Sensor Networks with Security Constraints. IEEE Transactions on Aerospace and Electronic Systems, vol. 53:2, 2017.	Uppsala
Guo X., Leong A.S., Dey S. Power allocation for distortion minimization in distributed estimation with security constraints. IEEE Workshop on	Uppsala

Signal Processing Advances in Wireless Communications, SPAWC, vol. 2014-October:October, 2014.	
Guo X., Leong A.S., Dey S. Power allocation for estimation outage minimization with secrecy outage constraints. 2016 Australian Communications Theory Workshop, AusCTW 2016, 2016.	Uppsala
Guo Z., Johansson K.H., Shi L. A study of packet-reordering integrity attack on remote state estimation. Chinese Control Conference, CCC, Vol. 2016-August, 2016.	KTH
Guo Z., Shi D., Johansson K.H., Shi L. Consequence Analysis of Innovation-based Integrity Attacks with Side Information on Remote State Estimation. IFAC-PapersOnLine, vol. 50:1, 2017.	KTH
Guo Z., Shi D., Johansson K.H., Shi L. Optimal Linear Cyber-Attack on Remote State Estimation. IEEE Transactions on Control of Network Systems, vol. 4:1, 2017.	KTH
Guo Z., Shi D., Johansson K.H., Shi L. Worst-case analysis of innovation-based linear attack on remote state estimation with resource constraint. 2016 IEEE 55th Conference on Decision and Control, CDC 2016, 2016.	KTH
Guo Z., Shi D., Johansson K.H., Shi L. Worst-case stealthy innovation-based linear attack on remote state estimation. Automatica, Vol. 89, 2018.	KTH
Gustafsson M.S. Constructing security: Reflections on the margins of a case study of the use of electronic identification in ICT platforms in schools. IFIP Advances in Information and Communication Technology, Vol. 421, 2014.	Linköping
Gustiene P., Gustas R. A method for data minimization personal information sharing. CEUR Workshop Proceedings, Vol. 1223, 2013.	Karlstad
Hagman K., Frisk L., Menezes J., Saha M.M. Cyber security measures in protection and control IEDs. IET Conference Publications, vol. 2016:CP671, 2016.	ABB
Hallgren P., Ochoa M., Sabelfeld A. Bettertimes privacy-assured outsourced multiplications for additively homomorphic encryption on finite fields. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9451, 2015.	Chalmers
Hallgren P., Ochoa M., Sabelfeld A. InnerCircle: A parallelizable decentralized privacy-preserving location proximity protocol. 2015 13th Annual Conference on Privacy, Security and Trust, PST 2015, 2015.	Chalmers
Hallgren P., Ochoa M., Sabelfeld A. MaxPace: Speed-constrained location queries. 2016 IEEE Conference on Communications and Network Security, CNS 2016, 2017.	Chalmers

Hallgren P.A., Mauritzson D.T., Sabelfeld A. GlassTube: A lightweight approach to web application integrity. PLAS 2013 - Proceedings of the 2013 ACM SIGPLAN Workshop on Programming Languages and Analysis for Security, Co-located with PLDI 2013, 2013.	Chalmers, Ericsson
Han G., Shen W., Duong T.Q., Guizani M., Hara T. A proposed security scheme against denial of service attacks in cluster-based wireless sensor networks. Security and Communication Networks, vol. 7:12, 2014.	Blekinge
Harirchi F., Yong S.Z., Jacobsen E., Ozay N. Active Model Discrimination with Applications to Fraud Detection in Smart Buildings. IFAC-PapersOnLine, vol. 50:1, 2017.	KTH
Harnesk D., Thapa D. Equipment-as-experience: A heidegger-based position of information security. 2016 International Conference on Information Systems, ICIS 2016, 2016.	Luleå
Harrison Dinniss H.A. The nature of objects: Targeting networks and the challenge of defining cyber military objectives. Israel Law Review, vol. 48:1, 2015.	FHS
Hartswood M., Jirotka M., Chenu-Abente R., Hume A., Giunchiglia F., Martucci L.A., Fischer-Hübner S. Privacy for peer profiling in collective adaptive systems. IFIP Advances in Information and Communication Technology, Vol. 457, 2015.	Karlstad
Hartung R.L., Hakansson A., Moradian E. A prescription for cyber physical systems. Procedia Computer Science, vol. 60:1, 2015.	KTH, Stockholm
Hausknecht D., Magazinius J., Sabelfeld A. May I?-content security policy endorsement for browser extensions. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9148, 2015.	Chalmers
He D., Kumar N., Zeadally S., Vinel A., Yang L.T. Efficient and Privacy-Preserving Data Aggregation Scheme for Smart Grid Against Internal Adversaries. IEEE Transactions on Smart Grid, vol. 8:5, 2017.	Halmstad
He Z., Hewage K., Voigt T. Arpeggio: A penetration attack on glossy networks. 2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking, SECON 2016, 2016.	SICS, Uppsala
He Z., Voigt T. Droplet: A new denial-of-service attack on low power wireless sensor networks. Proceedings - IEEE 10th International Conference on Mobile Ad-Hoc and Sensor Systems, MASS 2013, 2013.	SICS, Uppsala
Hedekvist P.O., Rieck C., Jaldehag K., Backefeldt J. Experimental data from NTP-monitoring and uncertainty estimation in nationwide network. Proceedings of the Annual Precise Time and Time Interval Systems and Applications Meeting, PTTI, Vol. 2014-January, 2014.	SP

Hedin D., Bello L., Sabelfeld A. Information-flow security for JavaScript and its APIs. Journal of Computer Security, vol. 24:2, 2016.	Chalmers, Mälardalen
Hedin D., Bello L., Sabelfeld A. Value-Sensitive Hybrid Information Flow Control for a JavaScript-Like Language. Proceedings of the Computer Security Foundations Workshop, Vol. 2015-September, 2015.	Chalmers, Mälardalen
Hedin D., Birgisson A., Bello L., Sabelfeld A. JSFlow: Tracking information flow in JavaScript and its APIs. Proceedings of the ACM Symposium on Applied Computing, 2014.	Chalmers
Hedin Y., Moradian E. Security in multi-agent systems. Procedia Computer Science, vol. 60:1, 2015.	Stockholm
Hedström K., Karlsson F., Kolkowska E. Social action theory for understanding information security non-compliance in hospitals the importance of user rationale. Information Management and Computer Security, vol. 21:4, 2013.	Örebro
Heickerö R. Cyber Terrorism: Electronic Jihad. Strategic Analysis, vol. 38:4, 2014.	FHS
Heickerö R. Industrial espionage and theft of information. European Conference on Information Warfare and Security, ECCWS, Vol. 2015-January, 2015.	FHS
Henda N.B. Generic and efficient attacker models in SPIN. 2014 International SPIN Symposium on Model Checking of Software, SPIN 2014 - Proceedings, 2014.	Ericsson
Henda N.B., Norrman K., Pfeffer K. Formal Verification of the Security for Dual Connectivity in LTE. Proceedings - 3rd FME Workshop on Formal Methods in Software Engineering, Formalise 2015, 2015.	Ericsson
Hendrickx J.M., Johansson K.H., Jungers R.M., Sandberg H., Sou K.C. Efficient computations of a security index for false data attacks in power networks. IEEE Transactions on Automatic Control, vol. 59:12, 2015.	Chalmers
Hesamzadeh M.R., Galland O., Biggar D.R. Short-run economic dispatch with mathematical modelling of the adjustment cost. International Journal of Electrical Power and Energy Systems, Vol. 58, 2014.	KTH
Heule S., Stefan D., Yang E.Z., Mitchell J.C., Russo A. IFC inside: Retrofitting languages with dynamic information flow control. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9036, 2015.	Chalmers
Hewage K., Raza S., Voigt T., Gomez F. An experimental study of attacks on the availability of Glossy. Computers and Electrical Engineering, vol. 41:C, 2015.	SICS, Uppsala

Hewage K.C., Raza S., Voigt T. Protecting Glossy-Based Wireless Networks from Packet Injection Attacks. Proceedings - 14th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2017, 2017.	SICS, Uppsala
Hiran R., Carlsson N., Gill P. Characterizing large-scale routing anomalies: A case study of the China telecom incident. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 7799 LNCS, 2013.	Linköping
Hiran R., Carlsson N., Shahmehri N. Collaborative framework for protection against attacks targeting BGP and edge networks. Computer Networks, Vol. 122, 2017.	Linköping
Hiran R., Carlsson N., Shahmehri N. Crowd-based detection of routing anomalies on the internet. 2015 IEEE Conference on Communications and NetworkSecurity, CNS 2015, 2015.	Linköping
Hiran R., Carlsson N., Shahmehri N. Does scale, size, and locality matter? Evaluation of collaborative BGP security mechanisms. 2016 IFIP Networking Conference (IFIP Networking) and Workshops, IFIP Networking 2016, 2016.	Linköping
Hiran R., Carlsson N., Shahmehri N. PrefiSec: A distributed alliance framework for collaborative BGP monitoring and prefix-based Security. Proceedings of the ACM Conference on Computer and Communications Security, vol. 2014-November:November, 2014.	Linköping
Hofbauer H., Alonso-Fernandez F., Bigun J., Uhl A. Experimental analysis regarding the influence of iris segmentation on the recognition rate. IET Biometrics, vol. 5:3, 2016.	Halmstad
Hofbauer H., Alonso-Fernandez F., Wild P., Bigun J., Uhl A. A ground truth for Iris segmentation. Proceedings - International Conference on Pattern Recognition, 2014.	Halmstad
Hoffmann H., Ramachandra P., Kovacs I.Z., Jorguseski L., Gunnarsson F., Kurner T. Potential of dynamic spectrum allocation in LTE macro networks. Advances in Radio Science, Vol. 13, 2015.	Ericsson
Holm H. A large-scale study of the time required to compromise a computer system. IEEE Transactions on Dependable and Secure Computing, vol. 11:1, 2014.	KTH
Holm H., Afridi K.K. An expert-based investigation of the Common Vulnerability Scoring System. Computers and Security, Vol. 53, 2015.	FOI, Stockholm
Holm H., Ekstedt M. Estimates on the effectiveness of web application firewalls against targeted attacks. Information Management and Computer Security, vol. 21:4, 2013.	KTH

Holm H., Flores W.R., Ericsson G. Cyber security for a Smart Grid - What about phishing?. 2013 4th IEEE/PES Innovative Smart Grid Technologies Europe, ISGT Europe 2013, 2013.	KTH
Holm H., Flores W.R., Nohlberg M., Ekstedt M. An empirical investigation of the effect of target-related information in phishing attacks. Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOCW, 2014.	FOI, KTH, Skövde
Holm H., Karresand M., Vidström A., Westring E. A survey of industrial control system testbeds. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9417, 2015.	FOI
Holm H., Korman M., Ekstedt M. A Bayesian network model for likelihood estimations of acquirement of critical software vulnerabilities and exploits. Information and Software Technology, Vol. 58, 2015.	KTH
Holm H., Shahzad K., Buschle M., Ekstedt M. P2CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language. IEEE Transactions on Dependable and Secure Computing, vol. 12:6, 2015.	KTH
Holm H., Sommestad T. So long, and thanks for only using readily available scripts. Information and Computer Security, vol. 25:1, 2017.	FOI
Holm H., Sommestad T. SVED: Scanning, Vulnerabilities, Exploits and Detection. Proceedings - IEEE Military Communications Conference MILCOM, 2016.	FOI
Holm H., Sommestad T., Ekstedt M., Honeth N. Indicators of expert judgement and their significance: An empirical investigation in the area of cyber security. Expert Systems, vol. 31:4, 2014.	KTH
Holm H., Sommestad T., Ekstedt M., Nordström L. CySeMoL: A tool for cyber security analysis of enterprises. IET Conference Publications, vol. 2013:615 CP, 2013.	KTH
Holst A., Bohlin M., Ekman J., Sellin O., Lindström B., Larsen S. Statistical anomaly detection for train fleets. AI Magazine, vol. 34:1, 2013.	KTH, SICS
Homem I. Coriander: A toolset for generating realistic android digital evidence datasets. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, Vol. 216, 2018.	Stockholm
Homem I., Dosis S., Popov O. LEIA: The Live Evidence Information Aggregator: Towards efficient cyber-law enforcement. 2013 World Congress on Internet Security, WorldCIS 2013, 2013.	Stockholm

Homem I., Kanter T., Rahmani R. Improving distributed forensics and incident response in loosely controlled networked environments. International Journal of Security and its Applications, vol. 10:1, 2016.	Stockholm
Hovsepyan A., Scandariato R., Joosen W. Is Newer Always Better?: The Case of Vulnerability Prediction Models. International Symposium on Empirical Software Engineering and Measurement, Vol. 08-09-September-2016, 2016.	Chalmers
Hu J., Vasilakos A.V. Energy Big Data Analytics and Security: Challenges and Opportunities. IEEE Transactions on Smart Grid, vol. 7:5, 2016.	Luleå
Hu L., Wang Z., Liu X., Vasilakos A.V., Alsaadi F.E. Recent advances on state estimation for power grids with unconventional measurements. IET Control Theory and Applications, vol. 11:18, 2017.	Luleå
Huang X., Craig P., Wang Q. Identity-based association protocols for wireless personal area networks. Proceedings - 15th IEEE International Conference on Computer and Information Technology, CIT 2015, 14th IEEE International Conference on Ubiquitous Computing and Communications, IUCC 2015, 13th IEEE International Conference on Dependable, Autonomic and Secure Computing, DASC 2015 and 13th IEEE International Conference on Pervasive Intelligence and Computing, PICom 2015, 2015.	Kristianstad
Huang X., Gao X., Yan Z. Security protocols in body sensor networks using visible light communications. International Journal of Communication Systems, vol. 29:16, 2016.	Chalmers
Hummen R., Shafagh H., Raza S., Voig T., Wehrle K. Delegation-based authentication and authorization for the IP-based Internet of Things. 2014 11th Annual IEEE International Conference on Sensing, Communication, and Networking, SECON 2014, 2014.	SICS, Uppsala
Hummen R., Ziegeldorf J.H., Shafagh H., Raza S., Wehrle K. Towards viable certificate-based authentication for the Internet of Things. HotWiSec 2013 - Proceedings of the 2013 ACM Workshop on Hot Topics on Wireless Network Security and Privacy, 2013.	SICS
Hussain D., Ross P., Bednar P. The perception of the benefits and drawbacks of internet usage by the elderly people. Lecture Notes in Information Systems and Organisation, Vol. 23, 2018.	Lund
Ibidunmoye O., Lakew E.B., Elmroth E. A Black-Box Approach for Detecting Systems Anomalies in Virtualized Environments. Proceedings - 2017 IEEE International Conference on Cloud and Autonomic Computing, ICCAC 2017, 2017.	Umeå
Ilková V., Ilka A. Legal Cybernetics: An Educational Perspective. IFAC-PapersOnLine, vol. 49:6, 2016.	Chalmers

Ilvonen I., Jussila J., Karkkainen H., Paivarinta T. Knowledge security risk management in contemporary companies - Toward a proactive approach. Proceedings of the Annual Hawaii International Conference on System Sciences, Vol. 2015-March, 2015.	Luleå
Iqbal A., Alobaidli H., Guimaraes M., Popov O. Sandboxing: Aid in digital forensic research. Proceedings of the 2015 Information Security Curriculum Development Conference, InfoSec CD 2015, 2015.	Stockholm
Iqbal A., Ekstedt M., Alobaidli H. Digital forensic readiness in critical infrastructures: A case of substation automation in the power sector. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, Vol. 216, 2018.	KTH
Iqbal S., Thapa D. Initial design principles for an educational, on-line information security laboratory. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8167 LNCS, 2013.	Luleå
Iqbal S., Thapa D., Awad A.I., Paivarinta T. Conceptual model of online pedagogical information security laboratory: Toward an ensemble artifact. Proceedings of the Annual Hawaii International Conference on System Sciences, Vol. 2015-March, 2015.	Luleå
Irshad A., Sher M., Nawaz O., Chaudhry S.A., Khan I., Kumari S. A secure and provable multi-server authenticated key agreement for TMIS based on Amin et al. scheme. Multimedia Tools and Applications, vol. 76:15, 2017.	Blekinge
Islam M.M., Lautenbach A., Sandberg C., Olovsson T. A risk assessment framework for automotive embedded systems. CPSS 2016 - Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security, Co-located with Asia CCS 2016, 2016.	Chalmers, Volvo
Izosimov V., Asvestopoulos A., Blomkvist O., Torngren M. Security-aware development of cyber-physical systems illustrated with automotive case study. Proceedings of the 2016 Design, Automation and Test in Europe Conference and Exhibition, DATE 2016, 2016.	KTH
Jaatun M.G., Cruzes D.S., Angulo J., Fischer-Hübner S. Accountability through transparency for cloud customers. Communications in Computer and Information Science, Vol. 581, 2016.	Karlstad
Jacobsson A., Boldt M., Carlsson B. A risk analysis of a smart home automation system. Future Generation Computer Systems, Vol. 56, 2016.	Blekinge, Malmö
Jacobsson A., Boldt M., Carlsson B. On the risk exposure of smart home automation systems. Proceedings - 2014 International Conference on Future Internet of Things and Cloud, FiCloud 2014, 2014.	Blekinge, Malmö

Jacobsson A., Davidsson P. Towards a model of privacy and security for smart homes. IEEE World Forum on Internet of Things, WF-IoT 2015 - Proceedings, 2015.	Malmö
Jaitner M., Kantola H. Countering threats - A comprehensive model for utilization of social media for security and law enforcement authorities. European Conference on Information Warfare and Security, ECCWS, Vol. 2014-January, 2014.	Karlstad
Jamthagen C., Lantz P., Hell M. A new instruction overlapping technique for anti-disassembly and obfuscation of x86 binaries. WATeR 2013 - Proceedings of the 2013 IEEE Workshop on Anti-Malware Testing Research, 2013.	Ericsson, Lund
Jandel M. Computational creativity for counterdeception in information fusion. Proceedings of the 16th International Conference on Information Fusion, FUSION 2013, 2013.	FOI
Jaradat O., Sljivo I., Habli I., Hawkins R. Challenges of Safety Assurance for Industry 4.0. Proceedings - 2017 13th European Dependable Computing Conference, EDCC 2017, 2017.	Mälardalen
Jiang K., Batina L., Eles P., Peng Z. Robustness analysis of real-time scheduling against differential power analysis attacks. Proceedings of IEEE Computer Society Annual Symposium on VLSI, ISVLSI, 2014.	Linköping
Jiang K., Eles P., Peng Z. Optimization of secure embedded systems with dynamic task sets. Proceedings -Design, Automation and Test in Europe, DATE, 2013.	Linköping
Jiang K., Eles P., Peng Z., Chattopadhyay S., Batina L. SPARTA: A scheduling policy for thwarting differential power analysis attacks. Proceedings of the Asia and South Pacific Design Automation Conference, ASP-DAC, Vol. 25-28-January-2016, 2016.	Linköping
Jiang K., Lifa A., Eles P., Peng Z., Jiang W. Energy-aware design of secure multi-mode real-time embedded systems with FPGA co-processors. ACM International Conference Proceeding Series, 2013.	Linköping
Jiang W., Jiang K., Zhang X., Ma Y. Energy aware real-time scheduling policy with guaranteed security protection. Proceedings of the Asia and South Pacific Design Automation Conference, ASP-DAC, 2014.	Linköping
Jiang W., Jiang K., Zhang X., Ma Y. Energy Optimization of Security-Critical Real-Time Applications with Guaranteed Security Protection. Journal of Systems Architecture, vol. 61:7, 2015.	Linköping
Jimenez E.C., Nakarmi P.K., Naslund M., Norrman K. Subscription identifier privacy in 5G systems. 2017 International Conference on Selected Topics in Mobile and Wireless Networking, MoWNeT 2017, 2017.	Ericsson, KTH

Jin H., Papadimitratos P. Proactive certificate validation for VANETs. IEEE Vehicular Networking Conference, VNC, 2017.	KTH
Jin H., Papadimitratos P. Resilient collaborative privacy for Location-Based services. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9417, 2015.	KTH
Jin H., Papadimitratos P. Resilient privacy protection for location-based services through decentralization. Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2017, 2017.	KTH
Johansson G. Producing correlated photons using superconducting circuits. 2013 Conference on Lasers and Electro-Optics Europe and International Quantum Electronics Conference, CLEO/Europe-IQEC 2013, 2013.	Chalmers
Johnson P., Gorton D., Lagerström R., Ekstedt M. Time between vulnerability disclosures: A measure of software product vulnerability. Computers and Security, Vol. 62, 2016.	KTH
Johnson P., Vernotte A., Gorton D., Ekstedt M., Lagerström R. Quantitative information security risk estimation using probabilistic attack graphs. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10224 LNCS, 2017.	KTH
Jonsson L.S., Priebe G., Bladh M., Svedin C.G. Voluntary sexual exposure online among Swedish youth - Social background, Internet behavior and psychosocial health. Computers in Human Behavior, Vol. 30, 2014.	Lund
Jost C., Mattsson J., Näslund M., Smeets B. Cryptography in an all encrypted world. Ericsson Review (English Edition), vol. 93:1, 2016.	Lund
Jämthagen C., Karlsson L., Stankovski P., Hell M. EavesROP: Listening for ROP payloads in data streams. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8783, 2014.	Lund
Jämthagen C., Lantz P., Hell M. Exploiting trust in deterministic builds. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9922 LNCS, 2016.	Ericsson, Lund
Jändel M., Svenson P., Johansson R. Fusing restricted information. FUSION 2014 - 17th International Conference on Information Fusion, 2014.	FOI

Kaati L., Johansson F., Forsman E. Semantic technologies for detecting names of new drugs on darknets. 2016 IEEE International Conference on Cybercrime and Computer Forensic, ICCCF 2016, 2016.	FOI, Uppsala
Kaati L., Shrestha A., Cohen K. Linguistic analysis of lone offender manifestos. 2016 IEEE International Conference on Cybercrime and Computer Forensic, ICCCF 2016, 2016.	FOI, Uppsala
Kajtazi M., Bulgurcu B. Information security policy compliance: An empirical study on escalation of commitment. 19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime, Vol. 3, 2013.	Linné
Kajtazi M., Bulgurcu B., Cavusoglu H., Benbasat I. Assessing sunk cost effect on employees' intentions to violate information security policies in organizations. Proceedings of the Annual Hawaii International Conference on System Sciences, 2014.	Linné
Kajtazi M., Cavusoglu H. Guilt proneness as a mechanism towards information security policy compliance. Proceedings of the 24th Australasian Conference on Information Systems, 2013.	Linné
Kajtazi M., Cavusoglu H., Benbasat I., Haftor D. Assessing self-justification as an antecedent of noncompliance with information security policies. Proceedings of the 24th Australasian Conference on Information Systems, 2013.	Linné
Kajtazi M., Kolkowska E., Bulgurcu B. New insights into understanding manager's intentions to overlook ISP violation in organizations through escalation of commitment factors. Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015, 2015.	Linné, Örebro
Kalavri V., Blackburn J., Varvello M., Papagiannaki K. Like a pack of wolves: Community structure of web trackers. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9631, 2016.	KTH
Kalliamvakou E., Weber J., Knauss A. Certification of open source software – A scoping review. IFIP Advances in Information and Communication Technology, Vol. 472, 2016.	Chalmers
Kamrani F., Luotsinen L.J., Lovlid R.A. Learning objective agent behavior using a data-driven modeling approach. 2016 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2016 - Conference Proceedings, 2017.	FOI
Kang K., Pang Z., Xu L.D., Ma L., Wang C. An interactive trust model for application market of the internet of things. IEEE Transactions on Industrial Informatics, vol. 10:2, 2014.	ABB

Kang K., Pang Z.-B., Wang C. Security and privacy mechanism for health internet of things. Journal of China Universities of Posts and Telecommunications, vol. 20:SUPPL -2, 2013.	ABB
Kannan A., Venkatesan K.G., Stagkopoulou A., Li S., Krishnan S., Rahman A. A novel cloud intrusion detection system using feature selection and classification. International Journal of Intelligent Information Technologies, vol. 11:4, 2015.	KTH, Linköping, Uppsala
Karegar F., Striecks C., Krenn S., Hörandner F., Lorünser T., Fischer-Hübner S. Opportunities and challenges of credential towards a metadata-privacy respecting identity provider. IFIP Advances in Information and Communication Technology, Vol. 498, 2016.	Karlstad
Karg S., Tichy M., Raschke A., Liebel G. Model-driven software engineering in the open ETCS project: Project experiences and lessons learned. Proceedings - 19th ACM/IEEE International Conference on Model Driven Engineering Languages and Systems, MODELS 2016, 2016.	Chalmers
Kargén U., Shahmehri N. Towards accurate binary correspondence using runtime-observed values. Proceedings - 2016 IEEE International Conference on Software Maintenance and Evolution, ICSME 2016, 2017.	Linköping
Karlsson F., Goldkuhl G., Hedström K. Practice-based discourse analysis of infosec policies. IFIP Advances in Information and Communication Technology, Vol. 455, 2015.	Linköping, Örebro
Karlsson F., Hedström K. End user development and information security culture. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8533 LNCS, 2014.	Linköping, Örebro
Karlsson F., Hedström K., Goldkuhl G. Practice-based discourse analysis of information security policies. Computers and Security, Vol. 67, 2017.	Linköping, Örebro
Karlsson F., Karlsson M., Åström J. Measuring employees' compliance - The importance of value pluralism. Information and Computer Security, vol. 25:3, 2017.	Örebro
Karlsson F., Kolkowska E., Hedström K., Frostenson M. Inter-organisational information sharing - Between a rock and a hard place. Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015, 2015.	Örebro
Karlsson F., Kolkowska E., Prenkert F. Inter-organisational information security: A systematic literature review. Information and Computer Security, vol. 24:5, 2016.	Örebro

Karlsson F., Åström J., Karlsson M. Information security culture state-of-the-art review between 2000 and 2013. Information and Computer Security, vol. 23:3, 2015.	Örebro
Karlsson L., Hell M. Enabling key migration between non-compatible TPM versions. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9824 LNCS, 2016.	Lund
Karlsson M., Clerwall C., Nord L. Do Not Stand Corrected: Transparency and Users' Attitudes to Inaccurate News and Corrections in Online Journalism. Journalism and Mass Communication Quarterly, vol. 94:1, 2017.	Karlstad, Mitt
Kavathatzopoulos I., Asai R. Methods for it security and privacy. Proceedings of the IADIS International Conference ICT, Society and Human Beings 2013, Proceedings of the IADIS International Conference e-Commerce 2013, 2013.	Uppsala
Kavathatzopoulos I., Asai R., Adams A.A., Murata K. Snowden's revelations and the attitudes of students at Swedish universities. Journal of Information, Communication and Ethics in Society, vol. 15:3, 2017.	Uppsala
Kazemi S., Abghari S., Lavesson N., Johnson H., Ryman P. Open data for anomaly detection in maritime surveillance. Expert Systems with Applications, vol. 40:14, 2013.	Blekinge
Kekely L., Kucera J., Pus V., Korenek J., Vasilakos A.V. Software defined monitoring of application protocols. IEEE Transactions on Computers, vol. 65:2, 2016.	Luleå
Khakpour N., Schwarz O., Dam M. Machine assisted proof of ARMv7 instruction level isolation properties. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8307 LNCS, 2013.	SICS
Khazaei S., Wikström D. Randomized partial checking revisited. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 7779 LNCS, 2013.	KTH
Khodaei M., Jin H., Papadimitratos P. Towards deploying a scalable & robust vehicular identity and credential management infrastructure. IEEE Vehicular Networking Conference, VNC, vol. 2015-January:January, 2015.	KTH
Khodaei M., Papadimitratos P. Evaluating on-demand pseudonym acquisition policies in Vehicular Communication systems. IoV-VoI 2016 - Proceedings of the 1st MobiHoc International Workshop on Internet of Vehicles and Vehicles of Internet, 2016.	KTH

Khodaei M., Papadimitratos P. The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems. IEEE Vehicular Technology Magazine, vol. 10:4, 2015.	KTH
Khrennikov A. Two-slit experiment: quantum and classical probabilities. Physica Scripta, vol. 90:7, 2015.	Linné
Kildal P.-S., Glazunov A.A., Carlsson J., Majidzadeh A. Cost-effective measurement setups for testing wireless communication to vehicles in reverberation chambers and anechoic chambers. 2014 IEEE Conference on Antenna Measurements and Applications, CAMA 2014, 2014.	Chalmers
Kim D., Bi J., Vasilakos A.V., Yeom I. Security of Cached Content in NDN. IEEE Transactions on Information Forensics and Security, vol. 12:12, 2017.	Luleå
Kim H., Broman D., Kang E., Lee E.A. An Architectural Mechanism for Resilient IoT Services. SafeThings 2017 - Proceedings of the 1st ACM International Workshop on the Internet of Safe Things, Part of SenSys 2017, 2017.	KTH
Kim H., Kang E., Lee E.A., Broman D. A toolkit for construction of authorization service infrastructure for the internet of things. Proceedings - 2017 IEEE/ACM 2nd International Conference on Internet-of-Things Design and Implementation, IoTDI 2017 (part of CPS Week), 2017.	KTH
King J., Awad A.I. A distributed security mechanism for Resource-Constrained IoT Devices. Informatica (Slovenia), vol. 40:1, 2016.	Luleå
Kish L.B., Granqvist C.-G. Enhanced usage of keys obtained by physical, unconditionally secure distributions. Fluctuation and Noise Letters, vol. 14:2, 2015.	Uppsala
Kish L.B., Granqvist C.G. Random-resistor-random-temperature Kirchhoff-Law-Johnson-Noise (RRRT-KLJN) key exchange. Metrology and Measurement Systems, vol. 23:1, 2016.	Uppsala
Kittichokechai K., Oechtering T.J., Skoglund M., Chia Y.-K. Secure Source Coding With Action-Dependent Side Information. IEEE Transactions on Information Theory, vol. 61:12, 2015.	KTH
Kleberger P., Nowdehi N., Olovsson T. Towards designing secure in-vehicle network architectures using community detection algorithms. IEEE Vehicular Networking Conference, VNC, vol. 2015-January:January, 2015.	Chalmers, Volvo
Kleberger P., Olovsson T. Protecting vehicles against unauthorised diagnostics sessions using trusted third parties. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8153 LNCS, 2013.	Chalmers

Kleberger P., Olovsson T. Securing vehicle diagnostics in repair shops. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8666 LNCS, 2014.	Chalmers
Klein G.O. Standardization of cryptographic techniques –The influence of the security agencies. IFIP Advances in Information and Communication Technology, Vol. 447, 2015.	Örebro
Knauss A., Berger C., Eriksson H. Towards state-of-the-art and future trends in testing of active safety systems. Proceedings - 2nd International Workshop on Software Engineering for Smart Cyber-Physical Systems, SEsCPS 2016, 2016.	Chalmers, Göteborg
Kolkowska E., Avatare Nöu A., Sjölinder M., Scandurra I. Socio-technical challenges in implementation of monitoring technologies in elderly care. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9755, 2016.	SICS, Örebro
Kolkowska E., Dhillon G. Organizational power and information security rule compliance. Computers and Security, Vol. 33, 2013.	Örebro
Kolkowska E., Karlsson F., Hedström K. Towards analysing the rationale of information security non-compliance: Devising a Value-Based Compliance analysis method. Journal of Strategic Information Systems, vol. 26:1, 2017.	Örebro
Kolomvakis N., Matthaiou M., Coldrey M. Massive MIMO in sparse channels. IEEE Workshop on Signal Processing Advances in Wireless Communications, SPAWC, vol. 2014-October:October, 2014.	Chalmers, Ericsson
Kominos C.G., Seyvet N., Vandikas K. Bare-metal, virtual machines and containers in OpenStack. Proceedings of the 2017 20th Conference on Innovations in Clouds, Internet and Networks, ICIN 2017, 2017.	Ericsson, Uppsala
Koochak Shooshtari M., Ahmadian-Attari M., Johansson T., Aref M.R. Cryptanalysis of McEliece cryptosystem variants based on quasi-cyclic low-density parity check codes. IET Information Security, vol. 10:4, 2016.	Lund
Korman M., Lagerström R., Ekstedt M. Modeling authorization in enterprise-wide contexts. CEUR Workshop Proceedings, Vol. 1497, 2015.	KTH
Korman M., Sommestad T., Hallberg J., Bengtsson J., Ekstedt M. Overview of Enterprise Information Needs in Information Security Risk Assessment. Proceedings . IEEE 18th international Enterprise Distributed object computing conference, vol. 2014-December:December, 2014.	FOI, KTH

Korman M., Välja M., Björkman G., Ekstedt M., Vernotte A., Lagerström R. Analyzing the effectiveness of attack countermeasures in a SCADA system. Proceedings - 2017 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, CPSR-SG 2017 (part of CPS Week), 2017.	KTH
Kostopoulos A., Sfakianakis E., Chochliouros I., Pettersson J.S., Krenn S., Tesfay W., Migliavacca A., Hörandner F. Towards the adoption of secure cloud identity services. ACM International Conference Proceeding Series, Vol. Part F130521, 2017.	Karlstad
Kounelis I., Baldini G., Muftic S., Loschner J. An architecture for secure m-commerce applications. Proceedings - 19th International Conference on Control Systems and Computer Science, CSCS 2013, 2013.	KTH
Kounelis I., Muftic S., Loschner J. Secure and privacy-enhanced e-mail system based on the concept of proxies. 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2014 - Proceedings, 2014.	KTH
Kowalski S., Andersson T., Windahl S. I am ok, the material's not: A transactional analysis of information security education material for swedish elementary school students. Communications in Computer and Information Science, Vol. 714, 2017.	Stockholm
Kulyk O., Marky K., Neumann S., Volkamer M. Introducing proxy voting to helios. Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016, 2016.	Karlstad
Kulyk O., Neumann S., Budurushi J., Volkamer M., Haenni R., Koenig R., Von Bergen P. Efficiency evaluation of cryptographic protocols for boardroom voting. Proceedings - 10th International Conference on Availability, Reliability and Security, ARES 2015, 2015.	Karlstad
Kulyk O., Neumann S., Marky K., Budurushi J., Volkamer M. Coercion-resistant proxy voting. Computers and Security, Vol. 71, 2017.	Karlstad
Kulyk O., Neumann S., Marky K., Volkamer M. Enabling vote delegation for boardroom voting. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10323 LNCS, 2017.	Karlstad
Kulyk O., Reinheimer B.M., Gerber P., Volk F., Volkamer M., Muhlhauser M. Advancing trust visualisations for wider applicability and user acceptance. Proceedings - 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 11th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Conference on Embedded Software and Systems, Trustcom/BigDataSE/ICESS 2017, 2017.	Karlstad
Kulyk O., Volkamer M. Efficiency comparison of various approaches in E-voting protocols. Lecture Notes in Computer Science (including	Karlstad

subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9604 LNCS, 2016.	
Kumar P., Braeken A., Gurtov A., Iinatti J., Ha P.H. Anonymous Secure Framework in Connected Smart Home Environments. IEEE Transactions on Information Forensics and Security, vol. 12:4, 2017.	Linköping
Kumar P., Gurtov A., Iinatti J., Sain M., Ha P.H. Access Control Protocol with Node Privacy in Wireless Sensor Networks. IEEE Sensors Journal, vol. 16:22, 2016.	Linköping
Kung E., Dey S., Shi L. Optimal Stealthy Attack under KL Divergence and Countermeasure with Randomized Threshold. IFAC-PapersOnLine, vol. 50:1, 2017.	Uppsala
Kung E., Dey S., Shi L. The performance and limitations of ϵ-stealthy attacks on higher order systems. IEEE Transactions on Automatic Control, vol. 62:2, 2017.	Uppsala
Kuźniar M., Perešíni P., Kostić D. What you need to know about SDN flow tables. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8995, 2015.	KTH
Kvarnbrink P., Fahlquist K., Mejtoft T. Biometric Interaction – A Case Study of Visual Feedback and Privacy Issues in New Face Recognition Solutions. Conference on Human Factors in Computing Systems - Proceedings, Vol. 2013-April, 2013.	Umeå
Lagerkvist A., Andersson Y. The grand interruption: death online and mediated lifelines of shared vulnerability. Feminist Media Studies, vol. 17:4, 2017.	Stockholm
Lagerstrom R., Johnson P., Ekstedt M. Automatic design of secure enterprise architecture: Work in progress paper. Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOCW, Vol. 2017-October, 2017.	KTH
Lagerström R., Baldwin C., MacCormack A., Sturtevant D., Doolan L. Exploring the relationship between architecture coupling and software vulnerabilities. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10379 LNCS, 2017.	KTH
Landegren F., Johansson J., Samuelsson O. Review of computer based approaches for modeling and simulating critical infrastructures as Socio-Technical Systems. Safety, Reliability and Risk Analysis: Beyond the Horizon - Proceedings of the European Safety and Reliability Conference, ESREL 2013, 2014.	Lund
Landsiedel O., Petig T., Schiller E.M. DecTDMA: A decentralized-TDMA with link quality estimation for WSNS. Lecture Notes in Computer	Chalmers

Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10083 LNCS, 2016.	
Lantz P., Johansson B., Hell M., Smeets B. Visual cryptography and obfuscation: A use-case for decrypting and deobfuscating information using augmented reality. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8976, 2015.	Ericsson, Lund
Larmuseau A., Patrignani M., Clarke D. A secure compiler for ML modules. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9458, 2015.	Uppsala
Larsson E., Zadegan F.G. Accessing on-chip instruments through the life-time of systems. LATS 2016 - 17th IEEE Latin-American Test Symposium, 2016.	Lund
Larsson M.B.-O., Björkman G., Ekstedt M. Assessment of social impact costs and social impact magnitude from breakdowns in critical infrastructures. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 7722 LNCS, 2013.	KTH
Laxhammar R., Falkman G. Online learning and sequential anomaly detection in trajectories. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 36:6, 2014.	Saab, Skövde
Lazar J., Abascal J., Barbosa S., Barksdale J., Friedman B., Grossklags J., Gulliksen J., Johnson J., McEwan T., Martínez-Normand L., Michalk W., Tsai J., Van Der Veer G., Von Axelson H., Walldius A., Whitney G., Winckler M., Wulf V., Churchill E.F., Cranor L., Davis J., Hedge A., Hochheiser H., Hourcade J.P., Lewis C., Nathan L., Paterno F., Reid B., Quesenbery W., Selker T., Wentz B. Human-computer interaction and international public policymaking: A framework for understanding and taking future actions. Foundations and Trends in Human-Computer Interaction, vol. 9:2, 2015.	KTH
Le A., Loo J., Lasebae A., Vinel A., Chen Y., Chai M. The impact of rank attack on network topology of routing protocol for low-power and lossy networks. IEEE Sensors Journal, vol. 13:10, 2013.	Halmstad
Lee C.-C., Li C.-T., Cheng C.-L., Lai Y.-M., Vasilakos A.V. A Novel Group Ownership Delegate Protocol for RFID Systems. Information Systems Frontiers, 2018.	Luleå
Lenhard J., Fritsch L., Herold S. A literature study on privacy patterns research. Proceedings - 43rd Euromicro Conference on Software Engineering and Advanced Applications, SEAA 2017, 2017.	Karlstad

Lennvall T., Gidlund M., Akerberg J. Challenges when bringing IoT into industrial automation. 2017 IEEE AFRICON: Science, Technology and Innovation for Africa, AFRICON 2017, 2017.	ABB, Mitt
Li H., Dán G., Nahrstedt K. FADEC: Fast authentication for dynamic electric vehicle charging. 2013 IEEE Conference on Communications and Network Security, CNS 2013, 2013.	KTH
Li H., Dán G., Nahrstedt K. Portunes: Privacy-preserving fast authentication for dynamic electric vehicle charging. 2014 IEEE International Conference on Smart Grid Communications, SmartGridComm 2014, 2015.	KTH
Li H., Dan G., Nahrstedt K. Portunes+: Privacy-Preserving Fast Authentication for Dynamic Electric Vehicle Charging. IEEE Transactions on Smart Grid, vol. 8:5, 2017.	KTH
Li N., Dubrova E. On-chip area-efficient binary sequence storage. Proceedings of the ACM Great Lakes Symposium on VLSI, GLSVLSI, 2013.	KTH
Li N., Mansouri S.S., Dubrova E. Secure key storage using state machines. Proceedings of The International Symposium on Multiple-Valued Logic, 2013.	KTH
Li X., Dai H.-N., Wang Q., Vasilakos A.V. AE-shelter: An novel anti-eavesdropping scheme in wireless networks. IEEE International Conference on Communications, 2017.	Luleå
Li Y., Pappas N., Angelakis V., Pioro M., Yuan D. Resilient topology design for free space optical cellular backhaul networking. 2014 IEEE Globecom Workshops, GC Wkshps 2014, 2014.	Linköping, Lund
Li Y., Quevedo D.E., Dey S., Shi L. Fake-acknowledgment attack on ACK-based sensor power schedule for remote state estimation. Proceedings of the IEEE Conference on Decision and Control, Vol. 54rd IEEE Conference on Decision and Control,CDC 2015, 2016.	Uppsala
Li Y., Quevedo D.E., Dey S., Shi L. SINR-Based DoS attack on remote state estimation: A game-theoretic approach. IEEE Transactions on Control of Network Systems, vol. 4:3, 2017.	Uppsala
Li Z., Oechtering T.J. Privacy-Aware Distributed Bayesian Detection. IEEE Journal on Selected Topics in Signal Processing, vol. 9:7, 2015.	KTH
Li Z., Oechtering T.J. Privacy-concerned parallel distributed Bayesian sequential detection. 2014 IEEE Global Conference on Signal and Information Processing, GlobalSIP 2014, 2014.	KTH
Li Z., Oechtering T.J., Skoglund M. Privacy-preserving energy flow control in smart grids. ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings, Vol. 2016-May, 2016.	KTH

Liang B., Mitrokotsa A. Fast and adaptively secure signatures in the random oracle model from indistinguishability obfuscation (short paper). Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10701 LNCS, 2017.	Chalmers
Lif P., Granasen M., Sommestad T. Development and validation of technique to measure cyber situation awareness. 2017 International Conference On Cyber Situational Awareness, Data Analytics And Assessment, Cyber SA 2017, 2017.	FOI
Lif P., Sommestad T. Human factors related to the performance of intrusion detection operators. Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015, 2015.	FOI
Lin C., He D., Kumar N., Choo K.-K.R., Vinel A., Huang X. Security and Privacy for the Internet of Drones: Challenges and Solutions. IEEE Communications Magazine, vol. 56:1, 2018.	Halmstad
Lindh M., Nolin J. Information We Collect: Surveillance and Privacy in the Implementation of Google Apps for Education. European Educational Research Journal, vol. 15:6, 2016.	Borås
Lindholm C., Notander J.P., Höst M. A case study on software risk analysis and planning in medical device development. Software Quality Journal, vol. 22:3, 2014.	Lund
Lisova E., Uhlemann E., Steiner W., Akerberg J., Bjorkman M. Risk evaluation of an ARP poisoning attack on clock synchronization for industrial applications. Proceedings of the IEEE International Conference on Industrial Technology, Vol. 2016-May, 2016.	Mälardalen
Lisova E., Uhlemann E., Steiner W., Akerberg J., Björkman M. A Survey of Security Frameworks Suitable for Distributed Control Systems. 2015 International Conference on Computing and Network Communications, CoCoNet 2015, 2016.	Mälardalen
Lisova E., Uhlemann E., Åkerberg J., Björkman M. Towards secure wireless TTEthernet for industrial process automation applications. 19th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA 2014, 2014.	Halmstad
Liu M., Mansouri S.S., Dubrova E. A faster shift register alternative to filter generators. Proceedings - 16th Euromicro Conference on Digital System Design, DSD 2013, 2013.	KTH
Liu Y., Sun Y., Ryoo J., Rizvi S., Vasilakos A.V. A survey of security and privacy challenges in cloud computing: Solutions and future directions. Journal of Computing Science and Engineering, vol. 9:3, 2015.	Luleå

Liwång H., Ringsberg J.W. Ship security analysis - The effect of ship speed and effective lookout. Proceedings of the International Conference on Offshore Mechanics and Arctic Engineering - OMAE, Vol. 0,0833333333333333, 2013.	Chalmers
Liyanage M., Ylianttila M., Gurtov A. Enhancing Security, Scalability and Flexibility of Virtual Private LAN Services. IEEE CIT 2017 - 17th IEEE International Conference on Computer and Information Technology, 2017.	Linköping
Liyanage M., Ylianttila M., Gurtov A. Fast Transmission Mechanism for Secure VPLS Architectures. IEEE CIT 2017 - 17th IEEE International Conference on Computer and Information Technology, 2017.	Linköping
Llewellynn T., Milagro M., Deniz O., Fricker S., Storkey A., Pazos N., Velikic G., Leufgen K., Dahyot R., Koller S., Goumas G., Leitner P., Dasika G., Wang L., Tutschku K. BONSEYES: Platform for open development of systems of artificial intelligence. ACM International Conference on Computing Frontiers 2017, CF 2017, 2017.	Blekinge
Lopez-Rojas E.A., Axelsson S. Using the RetSim fraud simulation tool to set thresholds for triage of retail fraud. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9417, 2015.	Blekinge
Lorentzen C., Fiedler M., Johnson H. On user perception of safety in online social networks. International Journal of Communication Networks and Distributed Systems, vol. 11:1, 2013.	Blekinge
Lorido-Botran T., Huerta S., Tomás L., Tordsson J., Sanz B. An unsupervised approach to online noisy-neighbor detection in cloud data centers. Expert Systems with Applications, Vol. 89, 2017.	Umeå
Lorünser T., Rodriguez C.B., Demirel D., Fischer-Hübner S., Groß T., Länger T., des Noes M., Pöhls H.C., Rozenberg B., Slamanig D. Towards a new paradigm for privacy and security in cloud services. Communications in Computer and Information Science, Vol. 530, 2015.	Karlstad
Lu X., de Lamare R.C., Zu K. Successive optimization Tomlinson-Harashima precoding strategies for physical-layer security in wireless networks. Eurasip Journal on Wireless Communications and Networking, vol. 2016:1, 2016.	Ericsson
Lu X., Zu K., De Lamare R.C. Lattice-reduction aided Successive Optimization Tomlinson-Harashima Precoding strategies for physical-layer security in wireless networks. 2014 Sensor Signal Processing for Defence, SSPD 2014, 2014.	Ericsson
Lundin P. Computers and welfare: The Swedish debate on the politics of computerization in the 1970s and the 1980s. IFIP Advances in Information and Communication Technology, Vol. 447, 2015.	Chalmers

Luotsinen L.J., Kamrani F., Hammar P., Jandel M., Lovlid R.A. Evolved creative intelligence for computer generated forces. 2016 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2016 - Conference Proceedings, 2017.	FOI
Löndahl C., Johansson T. Improved algorithms for finding low-weight polynomial multiples in F 2[x] and some cryptographic applications. Designs, Codes, and Cryptography, vol. 73:2, 2014.	Lund
Löndahl C., Johansson T., Koochak Shooshtari M., Ahmadian-Attari M., Aref M.R. Squaring attacks on McEliece public-key cryptosystems using quasi-cyclic codes of even dimension. Designs, Codes, and Cryptography, vol. 80:2, 2016.	Lund
Machackova H., Cerna A., Sevcikova A., Dedkova L., Daneback K. Effectiveness of coping strategies for victims of cyberbullying. Cyberpsychology, vol. 7:3, 2013.	Göteborg
Magazinius J., Hedin D., Sabelfeld A. Architectures for inlining security monitors in web applications. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8364 LNCS, 2014.	Chalmers
Magazinius J., Rios B.K., Sabelfeld A. Polyglots: Crossing origins by crossing formats. Proceedings of the ACM Conference on Computer and Communications Security, 2013.	Chalmers
Mahfouzi R., Aminifar A., Eles P., Peng Z., Villani M. Intrusion-damage assessment and mitigation in cyber-physical systems for control applications. ACM International Conference Proceeding Series, Vol. 19-21-October-2016, 2016.	Linköping
MallÃ©n A. Stirring up virtual punishment: a case of citizen journalism, authenticity and shaming. Journal of Scandinavian Studies in Criminology and Crime Prevention, vol. 17:1, 2016.	Lund
Mansouri S.S., Dubrova E. An improved hardware implementation of the grain-128a stream cipher. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 7839 LNCS, 2013.	KTH
Mansouri S.S., Dubrova E. Double-edge transformation for optimized power analysis suppression countermeasures. Proceedings - 16th Euromicro Conference on Digital System Design, DSD 2013, 2013.	KTH
Mansouri S.S., Dubrova E. Protecting ring oscillator physical unclonable functions against modeling attacks. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8565, 2014.	KTH
Mattsson J., Westerlund M. Authentication key recovery on Galois/Counter Mode (GCM). Lecture Notes in Computer Science	Ericsson

(including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9646, 2016.	
Mayer P., Gerber N., McDermott R., Volkamer M., Vogt J. Productivity vs security: Mitigating conflicting goals in organizations. Information and Computer Security, vol. 25:2, 2017.	Uppsala
Mayer P., Neumann S., Storck D., Volkamer M. Supporting decision makers in choosing suitable authentication schemes. Proceedings of the 10th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2016, 2016.	Karlstad
Mayer P., Neumann S., Volkamer M. POSTER: Towards collaboratively supporting decision makers in choosing suitable authentication schemes. Proceedings of the ACM Conference on Computer and Communications Security, Vol. 24-28-October-2016, 2016.	Karlstad
Mayer P., Volkamer M. Secure and efficient key derivation in portfolio authentication schemes using blakley secret sharing. ACM International Conference Proceeding Series, Vol. 7-11-December-2015, 2015.	Karlstad
McMillan D. Implicit interaction through machine learning: Challenges in design, accountability, and privacy. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10673 LNCS, 2017.	Stockholm
Mehri V.A., Tutschku K. Privacy and trust in cloud-based marketplaces for AI and data resources. IFIP Advances in Information and Communication Technology, Vol. 505, 2017.	Blekinge
Melrose J., Wrona K., Guenther T., Haakseth R., Nordbotten N., Westerdahl L. Labelling for integrity and availability. 2016 International Conference on Military Communications and Information Systems, ICMCIS 2016, 2016.	FOI
Metalidou E., Marinagi C., Trivellas P., Eberhagen N., Giannakopoulos G., Skourlas C. Human factor and information security in higher education. Journal of Systems and Information Technology, vol. 16:3, 2014.	Linné
Michalas A., Dowsley R. Towards Trusted eHealth Services in the Cloud. Proceedings - 2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing, UCC 2015, 2015.	SICS
Michalas A., Komninos N. The lord of the sense: A privacy preserving reputation system for participatory sensing applications. Proceedings - International Symposium on Computers and Communications, 2014.	SICS
Michalski A., Norman L. Conceptualizing European security cooperation: Competing international political orders and domestic factors. European Journal of International Relations, vol. 22:4, 2016.	Uppsala

Mikaelyan A., Alonso-Fernandez F., Bigun J. Periocular recognition by detection of local symmetry patterns. Proceedings - 10th International Conference on Signal-Image Technology and Internet-Based Systems, SITIS 2014, 2015.	Halmstad
Mikaelyan A., Bigun J. Symmetry assessment by finite expansion: Application to forensic fingerprints. Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI), Vol. P-230, 2014.	Halmstad
Miloševič J., Tanaka T., Sandberg H., Johansson K.H. Analysis and Mitigation of Bias Injection Attacks Against a Kalman Filter. IFAC-PapersOnLine, vol. 50:1, 2017.	KTH
Miloševic J., Tanaka T., Sandberg H., Johansson K.H. Exploiting Submodularity in Security Measure Allocation for Industrial Control Systems. SafeThings 2017 - Proceedings of the 1st ACM International Workshop on the Internet of Safe Things, Part of SenSys 2017, 2017.	KTH
Mingesz R., Kish L.B., Gingl Z., Granqvist C.G., Wen H., Peper F., Eubanks T., Schmera G. Information theoretic security by the laws of classical physics (plenary paper). Advances in Intelligent Systems and Computing, Vol. 195 AISC, 2013.	Uppsala
Mingesz R., Kish L.B., Gingl Z., Granqvist C.-G., Wen H., Peper F., Eubanks T., Schmera G. Unconditional security by the laws of classical physics. Metrology and Measurement Systems, vol. 20:1, 2013.	Uppsala
Mirmohseni M., Papadimitratos P. Colluding eavesdroppers in large cooperative wireless networks. IWCIT 2014 - Iran Workshop on Communication and Information Theory, 2014.	KTH
Mirmohseni M., Papadimitratos P.P. Secrecy capacity scaling in large cooperative wireless networks. IEEE Transactions on Information Theory, vol. 63:3, 2017.	KTH
Mitrokotsa A. Authentication in constrained settings. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9024, 2015.	Chalmers
Mitrokotsa A., Onete C., Vaudenay S. Location leakage in distance bounding: Why location privacy does not work. Computers and Security, Vol. 45, 2014.	Chalmers
Mohanty M., Ooi W.T., Atrey P.K. Secret sharing approach for securing cloud-based pre-classification volume ray-casting. Multimedia Tools and Applications, vol. 75:11, 2016.	SICS
Mohd B.J., Hayajneh T., Khalaf Z.A., Vasilakos A.V. A comparative study of steganography designs based on multiple FPGA platforms. International Journal of Electronic Security and Digital Forensics, vol. 8:2, 2016.	Luleå

Mohd B.J., Hayajneh T., Vasilakos A.V. A survey on lightweight block ciphers for low-resource devices: Comparative study and open issues. Journal of Network and Computer Applications, Vol. 58, 2015.	Luleå
Mollah M.B., Azad A.K., Vasilakos A. Secure data sharing and searching at the edge of cloud-assisted internet of things. IEEE Cloud Computing, vol. 4:1, 2017.	Luleå
Mollah M.B., Azad M.A.K., Vasilakos A. Security and privacy challenges in mobile cloud computing: Survey and way ahead. Journal of Network and Computer Applications, Vol. 84, 2017.	Luleå
Monshizadeh M., Khatri V., Gurtov A. NFV security considerations for cloud-based mobile virtual network operators. 2016 24th International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2016, 2016.	Linköping
Moosavi S.R., Gia T.N., Nigussie E., Rahmani A.M., Virtanen S., Tenhunen H., Isoaho J. End-to-end security scheme for mobility enabled healthcare Internet of Things. Future Generation Computer Systems, Vol. 64, 2016.	KTH
Moosavi S.R., Gia T.N., Nigussie E., Rahmani A.-M., Virtanen S., Tenhunen H., Isoaho J. Session resumption-based end-to-end security for healthcare internet-of-things. Proceedings - 15th IEEE International Conference on Computer and Information Technology, CIT 2015, 14th IEEE International Conference on Ubiquitous Computing and Communications, IUCC 2015, 13th IEEE International Conference on Dependable, Autonomic and Secure Computing, DASC 2015 and 13th IEEE International Conference on Pervasive Intelligence and Computing, PICom 2015, 2015.	KTH
Moosavi S.R., Gia T.N., Rahmani A.-M., Nigussie E., Virtanen S., Isoaho J., Tenhunen H. SEA: A secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. Procedia Computer Science, vol. 52:1, 2015.	KTH
Moradi M., Tao S., Mirzaee R.F. Physical Unclonable Functions Based on Carbon Nanotube FETs. Proceedings of The International Symposium on Multiple-Valued Logic, 2017.	KTH
Moradian E. Security of e-commerce software systems. Studies in Computational Intelligence, Vol. 462, 2013.	KTH
Mostowski W. Verifying java card programs. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10001 LNCS, 2016.	Halmstad
Mozelius P., Lesley C., Olsson O. IP-please, design and development of an educational game on IT-Security. Proceedings of the European Conference on Games-based Learning, Vol. 2016-January, 2016.	Stockholm

Mullner N., Khan S., Rahman M.H., Afzal W., Saadatmand M. Simulation-Based Safety Testing Brake-by-Wire. Proceedings - 10th IEEE International Conference on Software Testing, Verification and Validation Workshops, ICSTW 2017, 2017.	Mälardalen, SICS
Murdock V., Clarke C.L.A., Kamps J., Karlgren J. Second Workshop on Search and Exploration of X-Rated Information (SEXI'16): WSDM workshop summary. WSDM 2016 - Proceedings of the 9th ACM International Conference on Web Search and Data Mining, 2016.	KTH
Murray T., Sabelfeld A., Bauer L. Special issue on verified information flow security. Journal of Computer Security, vol. 25:43195, 2017.	Chalmers
Månsson A. A resource curse for renewables? Conflict and cooperation in the renewable energy sector. Energy Research and Social Science, Vol. 10, 2015.	Lund
Nagy A., Landsiedel O. Towards energy efficient, high-speed communication in WSNs. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8696 LNCS, 2014.	Göteborg
Nakarmi P.K., Ohlsson O., Liljenstam M. An air interface signaling protection function for mobile networks: GSM experiments and beyond. Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015, Vol. 1, 2015.	Ericsson
Nasim R., Buchegger S. XACML-based access control for decentralized online social networks. Proceedings - 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing, UCC 2014, 2014.	Karlstad, KTH
Naslund M., Dubrova E., Selander G., Lindqvist F. A random access procedure based on tunable puzzles. 2015 IEEE Conference on Communications and NetworkSecurity, CNS 2015, 2015.	Ericsson, KTH
Nawareg M., Muhammad S., Amselem E., Bourennane M. Experimental Measurement-Device-Independent Entanglement Detection. Scientific Reports, Vol. 5, 2015.	Stockholm
Nazir S., Shahzad S., Nazir M., Rehman H.U. Evaluating security of software components using analytic network process. Proceedings - 11th International Conference on Frontiers of Information Technology, FIT 2013, 2013.	Stockholm
Nelson B., Dimitrakakis C., Shi E. Summary/overview for artificial intelligence and security (AISec'13). Proceedings of the ACM Conference on Computer and Communications Security, 2013.	Chalmers
Nemati H., Dam M., Guanciale R., Do V., Vahidi A. Trustworthy memory isolation of linux on embedded devices. Lecture Notes in Computer	KTH

Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9229, 2015.	
Nešic D., Nyberg M., Gallina B. Modeling product-line legacy assets using multi-level theory. ACM International Conference Proceeding Series, Vol. 2, 2017.	KTH
Neumann S., Noll M., Volkamer M. Election-dependent security evaluation of internet voting schemes. IFIP Advances in Information and Communication Technology, Vol. 502, 2017.	Karlstad
Neumann S., Reinheimer B., Volkamer M. Don't be deceived: The message might be fake. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10442 LNCS, 2017.	Karlstad
Neumann S., Volkamer M., Budurushi J., Prandini M. SecIVo: a quantitative security evaluation framework for internet voting schemes. Annales des Telecommunications/Annals of Telecommunications, vol. 71:43289, 2016.	Karlstad
Ngai E., Ohlman B., Tsudik G., Uzun E., Wahlisch M., Wood C.A. Can we make a cake and eat it too? a discussion of icn security and privacy. Computer Communication Review, vol. 47:1, 2017.	Ericsson, Uppsala
Ngai E.C.-H. On providing sink anonymity for wireless sensor networks. Security and Communication Networks, vol. 9:2, 2016.	Uppsala
Nguyen P.H., Yskout K., Heyman T., Klein J., Scandariato R., Le Traon Y. SoSPa: A system of Security design Patterns for systematically engineering secure systems. 2015 ACM/IEEE 18th International Conference on Model Driven Engineering Languages and Systems, MODELS 2015 - Proceedings, 2015.	Chalmers, Göteborg
Niemimaa M., Laaksonen A.E., Harnesk D. Interpreting information security policy outcomes: A frames of Reference perspective. Proceedings of the Annual Hawaii International Conference on System Sciences, 2013.	Luleå
Nilsson A., Andersson M., Axelsson S. Key-hiding on the ARM platform. Digital Investigation, vol. 11:SUPPL. 1, 2014.	Blekinge
Nino J.-R., Enström G., Davidson A.R. Factors in fraudulent emails that deceive elderly people. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10297 LNCS, 2017.	Stockholm
Niu H., Zhu N., Sun L., Vasilakos A.V., Sezaki K. Security-embedded opportunistic user cooperation with full diversity. Wireless Networks, vol. 22:5, 2016.	Luleå
Niwa T., Miyazawa M., Hayashi M., Stadler R. Universal fault detection for NFV using SOM-based clustering. 17th Asia-Pacific Network	KTH

Operations and Management Symposium: Managing a Very Connected World, APNOMS 2015, 2015.	
Nordell V., Aurelius A., Gavler A., Arvidsson A., Kihl M. Concurrency and locality of content demand. 2013 International Conference on Smart Communications in Network Technologies, SaCoNeT 2013, Vol. 3, 2013.	Ericsson
Notzel J., Wiese M., Boche H. The Arbitrarily Varying Wiretap Channel-Secret Randomness, Stability, and Super-Activation. IEEE Transactions on Information Theory, vol. 62:6, 2016.	KTH
Nyberg A., Wiberg M. Sociala medier - ett nät av härskartekniker?. Human IT, vol. 13:1, 2015.	Umeå
O'Neill J., Dhareshwar A., Muralidhar S.H. Working Digital Money into a Cash Economy: The Collaborative Work of Loan Payment. Computer Supported Cooperative Work: CSCW: An International Journal, vol. 26:43196, 2017.	Chalmers
Okoh E., Awad A.I. Biometrics applications in e-health security: A preliminary survey. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9085, 2015.	Luleå
Okoh E., Makame M.H., Awad A.I. Toward online education for fingerprint recognition: A proof-of-concept web platform. Information Security Journal, vol. 26:4, 2017.	Luleå
Oluic M., Ghandhari M., Berggren B. Methodology for Rotor Angle Transient Stability Assessment in Parameter Space. IEEE Transactions on Power Systems, vol. 32:2, 2017.	KTH
Orue I., Andershed H. The Youth Psychopathic Traits Inventory-Short Version in Spanish Adolescents—Factor Structure, Reliability, and Relation with Aggression, Bullying, and Cyber Bullying. Journal of Psychopathology and Behavioral Assessment, vol. 37:4, 2015.	Örebro
Osman H., Van Zadelhoff A., Chaudron M.R.V. UML class diagram simplification: A survey for improving reverse engineered class diagram comprehension. MODELSWARD 2013 - Proceedings of the 1st International Conference on Model-Driven Engineering and Software Development, 2013.	Chalmers
Osman M.H., Chaudron M.R.V., Van Der Putten P. An analysis of machine learning algorithms for condensing reverse engineered class diagrams. IEEE International Conference on Software Maintenance, ICSM, 2013.	Chalmers
Ouvrier G., Laterman M., Arlitt M., Carlsson N. Characterizing the HTTPS trust landscape: A passive view from the edge. IEEE Communications Magazine, vol. 55:7, 2017.	Linköping

Padyab A., Päivärinta T., Ståhlbröst A., Bergvall-Kåreborn B. Facebook users attitudes towards secondary use of personal information. 2016 International Conference on Information Systems, ICIS 2016, 2016.	Luleå
Padyab A.M., Päivärinta T., Harnesk D. Genre-based approach to assessing information and knowledge security risks. International Journal of Knowledge Management, vol. 10:2, 2014.	Luleå
Padyab A.M., Päivärinta T., Harnesk D. Genre-based assessment of information and knowledge security risks. Proceedings of the Annual Hawaii International Conference on System Sciences, 2014.	Luleå
Pagnin E., Dimitrakakis C., Abidin A., Mitrokotsa A. On the leakage of information in biometric authentication. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8885, 2014.	Chalmers
Pagnin E., Hancke G., Mitrokotsa A. Using Distance-Bounding Protocols to Securely Verify the Proximity of Two-Hop Neighbours. IEEE Communications Letters, vol. 19:7, 2015.	Chalmers
Pagnin E., Mitrokotsa A. Privacy-Preserving Biometric Authentication: Challenges and Directions. Security and Communication Networks, Vol. 2017, 2017.	Chalmers
Pagnin E., Yang A., Hancke G., Mitrokotsa A. Short: HB+DB, mitigating man-in-the-middle attacks against HB+ with distance bounding. Proceedings of the 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec 2015, 2015.	Chalmers
Pagnin E., Yang A., Hu Q., Hancke G., Mitrokotsa A. HB+DB: Distance bounding meets human based authentication. Future Generation Computer Systems, Vol. 80, 2018.	Chalmers
Pahlberg T., Hagman O., Thurley M. Recognition of boards using wood fingerprints based on a fusion of feature detection methods. Computers and Electronics in Agriculture, Vol. 111, 2015.	Luleå
Paladi N., Aslam M., Gehrmann C. Trusted geolocation-aware data placement in infrastructure clouds. Proceedings - 2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2014, 2015.	Lund, SICS
Paladi N., Gehrmann C., Aslam M., Morenius F. Trusted launch of virtual machine instances in public IaaS environments. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 7839 LNCS, 2013.	Ericsson, SICS
Paladi N., Gehrmann C., Morenius F. Domain-Based Storage Protection (DBSP) in public infrastructure clouds. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8208 LNCS, 2013.	Ericsson, SICS

Paladi N., Michalas A. 'One of our hosts in another country': Challenges of data geolocation in cloud storage. 2014 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems, VITAE 2014 - Co-located with Global Wireless Summit, 2014.	Lund, SICS
Paladi N., Michalas A., Gehrmann C. Domain based storage protection with secure access control for the cloud. SCC 2014 - Proceedings of the 2nd International Workshop on Security in Cloud Computing, 2014.	SICS
Palm E. Conflicting Interests in the Development of a Harmonized EU e-Passport. Journal of Borderlands Studies, vol. 31:2, 2016.	Linköping
Pang Z., Chen Q., Tian J., Zheng L., Dubrova E. Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things. International Conference on Advanced Communication Technology, ICACT, 2013.	ABB, KTH
Pang Z., Yu K., Åkerberg J., Gidlund M. An RTOS-based architecture for industrial wireless sensor network stacks with multi-processor support. Proceedings of the IEEE International Conference on Industrial Technology, 2013.	Mälardalen
Pang Z., Zheng L., Tian J., Kao-Walter S., Dubrova E., Chen Q. Design of a terminal solution for integration of in-home health care devices and services towards the Internet-of-Things. Enterprise Information Systems, vol. 9:1, 2015.	ABB
Papakonstantinou N., Sierla S., Charitoudi K., O'Halloran B., Karhela T., Vyatkin V., Turner I. Security impact assessment of industrial automation systems using genetic algorithm and simulation. 19th IEEE International Conference on Emerging Technologies and Factory Automation, ETFA 2014, 2014.	Luleå
Papastergiou G., Grinnemo K.-J., Brunstrom A., Ros D., Töxen M., Khademi N., Hurtig P. On the cost of using happy eyeballs for transport protocol selection. ANRW 2016 - Proceedings of the ACM, IRTF and ISOC Applied Networking Research Workshop, 2016.	Karlstad
Pardo R., Balliu M., Schneider G. Formalising privacy policies in social networks. Journal of Logical and Algebraic Methods in Programming, Vol. 90, 2017.	Chalmers, Göteborg
Pardo R., Colombo C., Pace G.J., Schneider G. An automata-based approach to evolving privacy policies for social networks. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10012 LNCS, 2016.	Göteborg
Paridari K., Mady A.E.-D., La Porta S., Chabukswar R., Blanco J., Teixeira A., Sandberg H., Boubekeur M. Cyber-Physical-Security Framework for	KTH

Building Energy Management System. 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems, ICCPS 2016 - Proceedings, 2016.	
Park G., Shim H., Lee C., Eun Y., Johansson K.H. When adversary encounters uncertain cyber-physical systems: Robust zero-dynamics attack with disclosure resources. 2016 IEEE 55th Conference on Decision and Control, CDC 2016, 2016.	KTH
Peeters R., Pulls T. Insynd: Improved privacy-preserving transparency logging. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9879 LNCS, 2016.	Karlstad
Pereira D., Hirata C., Pagliares R., Nadjm-Tehrani S. Towards combined safety and security constraints analysis. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10489 LNCS, 2017.	Linköping
Pereira P.P., Eliasson J., Delsing J. An authentication and access control framework for CoAP-based Internet of Things. IECON Proceedings (Industrial Electronics Conference), 2014.	Luleå
Perera C., Vasilakos A. Privacy mindset for developing internet of things applications for social sensing: Software engineering challenges. Proceedings - 2017 2nd International Workshop on Social Sensing, SocialSens 2017 (part of CPS Week), 2017.	Luleå
Petrosyan V., Proutiere A. Viral clustering: A robust method to extract structures in heterogeneous datasets. 30th AAAI Conference on Artificial Intelligence, AAAI 2016, 2016.	KTH
Pettersson J.S. A brief evaluation of icons in the first reading of the European parliament on COM (2012) 0011. IFIP Advances in Information and Communication Technology, Vol. 457, 2015.	Karlstad
Phung P.H., Monshizadeh M., Sridhar M., Hamlen K.W., Venkatakrishnan V.N. Between Worlds: Securing Mixed JavaScript/ActionScript Multi-Party Web Content. IEEE Transactions on Dependable and Secure Computing, vol. 12:4, 2015.	Göteborg
Picazo-Sanchez P., Pardo R., Schneider G. Secure photo sharing in social networks. IFIP Advances in Information and Communication Technology, Vol. 502, 2017.	Chalmers, Göteborg
Pinol O.P., Raza S., Eriksson J., Voigt T. BSD-based elliptic curve cryptography for the open Internet of Things. 2015 7th International Conference on New Technologies, Mobility and Security - Proceedings of NTMS 2015 Conference and Workshops, 2015.	Uppsala
Porambage P., Ylianttila M., Schmitt C., Kumar P., Gurtov A., Vasilakos A.V. The Quest for Privacy in the Internet of Things. IEEE Cloud Computing, vol. 3:2, 2016.	Luleå

Poturalski M., Papadimitratos P., Hubaux J.-P. Formal analysis of secure neighbor discovery in wireless networks. IEEE Transactions on Dependable and Secure Computing, vol. 10:6, 2013.	KTH
Pozzoli T., Gini G., Thornberg R. Bullying and defending behavior: The role of explicit and implicit moral cognition. Journal of School Psychology, Vol. 59, 2016.	Linköping
Priebe G., Mitchell K.J., Finkelhor D. To tell or not to tell? Youth's responses to unwanted internet experiences. Cyberpsychology, vol. 7:1, 2013.	Linné
Pulls T., Peeters R., Wouters K. Distributed privacy-preserving transparency logging. Proceedings of the ACM Conference on Computer and Communications Security, 2013.	Karlstad
Pulls T., Slamanig D. On the feasibility of (practical) commercial anonymous cloud storage. Transactions on Data Privacy, vol. 8:2, 2015.	Karlstad
Punal O., Aktas I., Schnelke C.-J., Abidin G., Wehrle K., Gross J. Machine learning-based jamming detection for IEEE 802.11: Design and experimental evaluation. Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, WoWMoM 2014, 2014.	KTH
Purra J., Carlsson N. Third-Party Tracking on the Web: A Swedish Perspective. Proceedings - Conference on Local Computer Networks, LCN, 2016.	Linköping
Pöhls H.C., Angelakis V., Suppan S., Fischer K., Oikonomou G., Tragos E.Z., Rodriguez R.D., Mouroutis T. RERUM: Building a reliable IoT upon privacy- and security- enabled smart objects. 2014 IEEE Wireless Communications and Networking Conference Workshops, WCNCW 2014, 2014.	Linköping
Qinghua W. Using secret spreading codes to enhance physical layer security in wireless communication. 2017 IEEE International Conference on Communications Workshops, ICC Workshops 2017, 2017.	Kristianstad
Raciti M., Nadjm-Tehrani S. Embedded cyber-physical anomaly detection in smart meters. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 7722 LNCS, 2013.	Linköping
Rafnsson W., Garg D., Sabelfeld A. Progress-sensitive security for SPARK. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9639, 2016.	Chalmers

Rafnsson W., Nakata K., Sabelfeld A. Securing class initialization in java-like languages. IEEE Transactions on Dependable and Secure Computing, vol. 10:1, 2013.	Chalmers
Rahman H., Ahmed M.U., Begum S. Deep Learning Based Person Identification Using Facial Images. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, Vol. 225, 2018.	Mälardalen
Rajagopalan S., Upadhyay H.N., Ragavan R., Amirtharajan R., Rayappan J.B.B. Layer router for grayscale STEGO - A hardware architecture on FPGA and ASIC platforms. Journal of Scientific and Industrial Research, vol. 73:11, 2014.	Linköping
Rasmusson L., Nasab M.R. Hypervisor integrity measurement assistant. CLOSER 2013 - Proceedings of the 3rd International Conference on Cloud Computing and Services Science, 2013.	Chalmers, SICS
Ray A., Akerberg J., Bjorkman M., Blom R., Gidlund M. Applicability of LTE Public Key Infrastructure Based Device Authentication in Industrial Plants. Proceedings - International Computer Software and Applications Conference, Vol. 2, 2015.	ABB, Mitt, Mälardalen, SICS
Ray A., Akerberg J., Bjorkman M., Gidlund M. Balancing network performance and network security in a smart grid application. IEEE International Conference on Industrial Informatics (INDIN), 2017.	Mitt, Mälardalen
Ray A., Akerberg J., Bjorkman M., Gidlund M. Future research challenges of secure heterogeneous industrial communication networks. IEEE International Conference on Emerging Technologies and Factory Automation, ETFA, Vol. 2016-November, 2016.	ABB, Mitt, Mälardalen
Ray A., Akerberg J., Gidlund M., Bjorkman M. A solution for industrial device commissioning along with the initial trust establishment. IECON Proceedings (Industrial Electronics Conference), 2013.	ABB, Mälardalen
Ray A., Åkerberg J., Björkman M., Gidlund M. POSTER: An approach to assess security, capacity and reachability for heterogeneous industrial networks. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, Vol. 164, 2015.	ABB, Mitt, Mälardalen
Ray A., Åkerberg J., Gidlund M., Björkman M. Initial key distribution for industrial wireless sensor networks. Proceedings of the IEEE International Conference on Industrial Technology, 2013.	ABB, Mälardalen
Raza A., Morogan M.C., Mirza A.A., Mahmud M. Security analysis and countermeasures of current smart phones applications. Information (Japan), vol. 16:0,125, 2013.	Stockholm
Raza S., Duquennoy S., Höglund J., Roedig U., Voigt T. Secure communication for the Internet of Things-a comparison of link-layer	SICS

security and IPsec for 6LoWPAN. Security and Communication Networks, vol. 7:12, 2014.	
Raza S., Helgason T., Papadimitratos P., Voigt T. SecureSense: End-to-end secure communication architecture for the cloud-connected Internet of Things. Future Generation Computer Systems, Vol. 77, 2017.	KTH, Uppsala
Raza S., Seitz L., Sitenkov D., Selander G. S3K: Scalable Security with Symmetric Keys - DTLS Key Establishment for the Internet of Things. IEEE Transactions on Automation Science and Engineering, vol. 13:3, 2016.	Ericsson, SICS
Raza S., Shafagh H., Hewage K., Hummen R., Voigt T. Lithe: Lightweight secure CoAP for the internet of things. IEEE Sensors Journal, vol. 13:10, 2013.	SICS, Uppsala
Raza S., Wallgren L., Voigt T. SVELTE: Real-time intrusion detection in the Internet of Things. Ad Hoc Networks, vol. 11:8, 2013.	SICS, Uppsala
Rázuri J.G., Sundgren D., Rahmani R., Larsson A. Effect of emotional feedback in a decision-making system for an autonomous agent. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8864, 2014.	Stockholm
Rechert K., Meier K., Zahoransky R., Wehrle D., Von Suchodoletz D., Greschbach B., Wohlgemuth S., Echizen I. Reclaiming location privacy in mobile telephony networks-effects and consequences for providers and subscribers. IEEE Systems Journal, vol. 7:2, 2013.	KTH
Rho S., Vasilakos A.V., Chen W. Cyber-physical systems technologies and application - Part II. Future Generation Computer Systems, Vol. 61, 2016.	Luleå
Ribeiro E., Uhl A., Alonso-Fernandez F., Farrugia R.A. Exploring deep learning image super-resolution for iris recognition. 25th European Signal Processing Conference, EUSIPCO 2017, Vol. 2017-January, 2017.	Halmstad
Rigaki M., Elragal A. Adversarial deep learning against intrusion detection classifiers. CEUR Workshop Proceedings, Vol. 2057, 2017.	Luleå
Riveiro M., Lebram M., Elmer M. Anomaly detection for road traffic: A visual analytics framework. IEEE Transactions on Intelligent Transportation Systems, vol. 18:8, 2017.	Skövde, Volvo
Rizothanasis G., Carlsson N., Mahanti A. Identifying User Actions from HTTP(S) Traffic. Proceedings - Conference on Local Computer Networks, LCN, 2016.	Linköping
Robinson C. Disclosure of personal data in ecommerce: A cross-national comparison of Estonia and the United States. Telematics and Informatics, vol. 34:2, 2017.	Linköping

Rocha Flores W., Antonsen E., Ekstedt M. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers and Security, Vol. 43, 2014.	KTH
Rocha Flores W., Ekstedt M. Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Computers and Security, Vol. 59, 2016.	KTH
Rocha Flores W., Holm H., Svensson G., Ericsson G. Using phishing experiments and scenario-based surveys to understand security behaviours in practice. Information Management and Computer Security, vol. 22:4, 2014.	KTH
Rodgers W., Söderbom A., Guiral A. Corporate Social Responsibility Enhanced Control Systems Reducing the Likelihood of Fraud. Journal of Business Ethics, vol. 131:4, 2015.	Halmstad
Rodhe I., Bengtsson J., Hunstad A., Karlzen H. Future Schemes for Stronger Verification of the Access Rights of Border Control Inspection Systems. Proceedings - 2015 European Intelligence and Security Informatics Conference, EISIC 2015, 2016.	FOI
Rodríguez-Cano G., Greschbach B., Buchegger S. Event invitations in privacy-preserving DOSNs formalization and protocol design. IFIP Advances in Information and Communication Technology, Vol. 457, 2015.	KTH, Stockholm
Rojas M.A.T., Gonzalez N.M., Sbampato F.V., Redigolo F.F., Carvalho T., Ullah K.W., Naslund M., Ahmed A.S. A framework to orchestrate security SLA lifecycle in cloud computing. Iberian Conference on Information Systems and Technologies, CISTI, Vol. 2016-July, 2016.	Ericsson
Rojas M.A.T., Redígolo F.F., Gonzalez N.M., Sbampato F.V., De Brito Carvalho T.C.M., Ullah K.W., Näslund M., Ahmed A.S. Managing the lifecycle of security SLA requirements in cloud computing. Studies in Computational Intelligence, Vol. 718, 2018.	Ericsson
Rossebo J.E.Y., Wolthuis R., Fransen F., Bjorkman G., Medeiros N. An Enhanced Risk-Assessment Methodology for Smart Grids. Computer, vol. 50:4, 2017.	KTH
Ruebsamen T., Pulls T., Reich C. Secure evidence collection and storage for cloud accountability audits. CLOSER 2015 - 5th International Conference on Cloud Computing and Services Science, Proceedings, 2015.	Karlstad
Ruffa C., Vennesson P. Fighting and helping? A historical-institutionalist explanation of NGO-military relations. Security Studies, vol. 23:3, 2014.	FHS

Russo A. Functional pearl: Two can keep a secret, if one of them uses Haskell. Proceedings of the ACM SIGPLAN International Conference on Functional Programming, ICFP, Vol. 2015-August, 2015.	Chalmers
Rübsamen T., Pulls T., Reich C. Security and privacy preservation of evidence in cloud accountability audits. Communications in Computer and Information Science, Vol. 581, 2016.	Karlstad
Rögnvaldsson T., Norrman H., Byttner S., Järpe E. Estimating p-Values for Deviation Detection. International Conference on Self-Adaptive and Self-Organizing Systems, SASO, vol. 2014-December:December, 2014.	Halmstad
Sabbagh B.A., Kowalski S. A new socio-technical framework studies software supply chain security problems from a systemic viewpoint. It addresses three main issues: Modeling the target system, identifying threats, and analyzing countermeasures. IEEE Security and Privacy, vol. 13:4, 2015.	Stockholm
Sadeghi S., Bagheri N., Abdelraheem M.A. Cryptanalysis of reduced QTL block cipher. Microprocessors and Microsystems, Vol. 52, 2017.	SICS
Sadok M., Bednar P. Understanding security practices deficiencies: A contextual analysis. Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015, 2015.	Lund
Sahebi G., Majd A., Ebrahimi M., Plosila J., Karimpour J., Tenhunen H. SEECC: A secure and efficient elliptic curve cryptosystem for E-health applications. 2016 International Conference on High Performance Computing and Simulation, HPCS 2016, 2016.	KTH
Saleem S., Popov O., Appiah-Kubi O.K. Evaluating and comparing tools for mobile device forensics using quantitative analysis. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, Vol. 114 LNICST, 2013.	Stockholm
Saleem S., Popov O., Bagilli I. Extended abstract digital forensics model with preservation and protection as umbrella principles. Procedia Computer Science, vol. 35:C, 2014.	Stockholm
Salimi S., Jorswieck E.A., Skoglund M., Papadimitratos P. Key agreement over an interference channel with noiseless feedback: Achievable region & distributed allocation. 2015 IEEE Conference on Communications and NetworkSecurity, CNS 2015, 2015.	KTH
Sandberg H., Amin S., Johansson K.H. Cyberphysical security in networked control systems: An introduction to the issue. IEEE Control Systems, vol. 35:1, 2015.	KTH
Sandberg H., Teixeira A.M.H. From control system security indices to attack identifiability. 2016 Science of Security for Cyber-Physical Systems Workshop, SOSCYPS 2016, 2016.	KTH

Satta R., Stirparo P. Picture-to-identity linking of social network accounts based on sensor pattern noise. 5th International Conference on Imaging for Crime Detection and Prevention, ICDP 2013, 2013.	KTH
Saxena N., Grijalva S., Chukwuka V., Vasilakos A.V. Network Security and Privacy Challenges in Smart Vehicle-to-Grid. IEEE Wireless Communications, vol. 24:4, 2017.	Luleå
Sayaf R., Clarke D., Harper R. CPS2: A contextual privacy framework for social software. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, Vol. 153, 2015.	Uppsala
Sayaf R., Clarke D., Rule J.B. The other side of privacy: Surveillance in data control. ACM International Conference Proceeding Series, 2015.	Uppsala
Schoepe D., Balliu M., Pierce B.C., Sabelfeld A. Explicit secrecy: A policy for taint tracking. Proceedings - 2016 IEEE European Symposium on Security and Privacy, EURO S and P 2016, 2016.	Chalmers
Schoepe D., Balliu M., Piessens F., Sabelfeld A. Let's face it: Faceted values for taint tracking. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9878 LNCS, 2016.	Chalmers
Schoepe D., Hedin D., Sabelfeld A. SeLINQ: Tracking information across application-database boundaries. Proceedings of the ACM SIGPLAN International Conference on Functional Programming, ICFP, 2014.	Chalmers
Schougaard D., Dragoni N., Spognardi A. Evaluation of professional cloud password management tools. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9881 LNCS, 2016.	Örebro
Schwarz O., Dam M. Formal verification of secure user mode device execution with DMA. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8855, 2014.	SICS
Seepers R.M., Strydis C., Sourdis I., De Zeeuw C.I. Adaptive entity-identifier generation for IMD emergency access. ACM International Conference Proceeding Series, 2014.	Chalmers
Seepers R.M., Strydis C., Sourdis I., De Zeeuw C.I. On using a von neumann extractor in heart-beat-based security. Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015, Vol. 1, 2015.	Chalmers
Seepers R.M., Weber J.H., Erkin Z., Sourdis I., Strydis C. Secure key-exchange protocol for implants using heartbeats. 2016 ACM International Conference on Computing Frontiers - Proceedings, 2016.	Chalmers

Sequeira A.F., Chen L., Ferryman J., Alonso-Fernandez F., Bigun J., Raja K.B., Raghavendra R., Busch C., Wild P. Cross-Eyed-Cross-spectral Iris/Periocular Recognition database and competition. Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI), Vol. P-260, 2016.	Halmstad
Shafagh H., Hithnawi A., Drescher A., Duquennoy S., Hu W. Towards encrypted query processing for the Internet of Things. Proceedings of the Annual International Conference on Mobile Computing and Networking, MOBICOM, Vol. 2015-September, 2015.	SICS
Shafagh H., Hithnawi A., Dröscher A., Duquennoy S., Hu W. Talos: Encrypted query processing for the Internet of Things. SenSys 2015 - Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems, 2015.	SICS
Shahid A., Machuca C.M., Wosinska L., Chen J. Comparative analysis of protection schemes for fixed mobile converged access networks based on hybrid PON. CTTE 2015 - 2015 Conference of Telecommunication, Media and Internet Techno-Economics, Proceedings, 2015.	KTH
Shahzad R.K., Fatima M., Lavesson N., Boldt M. Consensus decision making in random forests. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9432, 2015.	Blekinge
Shahzad R.K., Lavesson N. Comparative analysis of voting schemes for ensemble-based malware detection. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 4:1, 2013.	Blekinge
Sharif S., Watson P., Taheri J., Nepal S., Zomaya A.Y. Privacy-Aware Scheduling SaaS in High Performance Computing Environments. IEEE Transactions on Parallel and Distributed Systems, vol. 28:4, 2017.	Karlstad
Shi D., Guo Z., Johansson K.H., Shi L. Causality Countermeasures for Anomaly Detection in Cyber-Physical Systems. IEEE Transactions on Automatic Control, vol. 63:2, 2018.	KTH
Shibli M.A., Masood R., Ghazi Y., Muftic S. MagicNET: Mobile agents data protection system. Transactions on Emerging Telecommunications Technologies, vol. 26:5, 2015.	KTH
Shokri R., Theodorakopoulos G., Papadimitratos P., Kazemi E., Hubaux J.-P. Hiding in the mobile crowd: Location privacy through collaboration. IEEE Transactions on Dependable and Secure Computing, vol. 11:3, 2014.	KTH
Shoukry Y., Araujo J., Tabuada P., Srivastava M., Johansson K.H. Minimax control for cyber-physical systems under network packet scheduling attacks. HiCoNS 2013 - Proceedings of the 2nd ACM	KTH

International Conference on High Confidence Networked Systems, Part of CPSWeek 2013, 2013.	
Shreenivas D., Raza S., Voigt T. Intrusion detection in the RPL-connected 6LoWPAN Networks. IoTPTS 2017 - Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, co-located with ASIA CCS 2017, 2017.	Ericsson
Shu Z., Wan J., Li D., Lin J., Vasilakos A.V., Imran M. Security in Software-Defined Networking: Threats and Countermeasures. Mobile Networks and Applications, vol. 21:5, 2016.	Luleå
Sï¿½ilen K.S. Economic and industrial espionage at the start of the 21st century - Status quaestionis. Journal of Intelligence Studies in Business, vol. 6:3, 2016.	Halmstad
Siddiquee K.N.E.A., Andersson K., Khan F.F., Hossain M.S. A scalable and secure MANET for an i-Voting system. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 8:3, 2017.	Luleå
Sierla S., Hurkala M., Charitoudi K., Yang C.-W., Vyatkin V. Security risk analysis for smart grid automation. IEEE International Symposium on Industrial Electronics, 2014.	Luleå
Sigholm J., Bang M. Towards Offensive cyber counterintelligence: Adopting a target-centric view on advanced persistent threats. Proceedings - 2013 European Intelligence and Security Informatics Conference, EISIC 2013, 2013.	FHS
Sigholm J., Larsson E. Determining the utility of cyber vulnerability implantation: The heartbleed bug as a cyber operation. Proceedings - IEEE Military Communications Conference MILCOM, 2014.	FHS
Simplicio Jr. M.A., De Oliveira B.T., Margi C.B., Barreto P.S.L.M., Carvalho T.C.M.B., Näslund M. Survey and comparison of message authentication solutions on wireless sensor networks. Ad Hoc Networks, vol. 11:3, 2013.	Ericsson
Sion L., Yskout K., Scandariato R., Joosen W. A modular meta-model for security solutions. ACM International Conference Proceeding Series, Vol. Part F129681, 2017.	Göteborg
Sion L., Yskout K., Van Den Berghe A., Scandariato R., Joosen W. MASC: Modelling architectural security concerns. Proceedings - 7th International Workshop on Modeling in Software Engineering, MiSE 2015, 2015.	Göteborg
Slonje R., Smith P.K., Frisén A. Perceived reasons for the negative impact of cyberbullying and traditional bullying. European Journal of Developmental Psychology, vol. 14:3, 2017.	Göteborg

Slonje R., Smith P.K., Frisén A. The nature of cyberbullying, and strategies for prevention. Computers in Human Behavior, vol. 29:1, 2013.	Göteborg
Snickars P. More of the same - On spotify radio. Culture Unbound, vol. 9:2, 2017.	Umeå
Soderberg A., Johansson R. Safety contract based design of software components. 2013 IEEE International Symposium on Software Reliability Engineering Workshops, ISSREW 2013, 2013.	SP
Solaiman E., Ranjan R., Jayaraman P.P., Mitra K. Monitoring Internet of Things Application Ecosystems for Failure. IT Professional, vol. 18:5, 2016.	Luleå
Somarriba O., Zurutuza U., Uribeetxeberria R., Delosiï¿½res L., Nadjm-Tehrani S. Detection and Visualization of Android Malware Behavior. Journal of Electrical and Computer Engineering, Vol. 2016, 2016.	Linköping
Sommestad T. Social groupings and information security obedience within organizations. IFIP Advances in Information and Communication Technology, Vol. 455, 2015.	FOI
Sommestad T., Ekstedt M., Holm H. The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures. IEEE Systems Journal, vol. 7:3, 2013.	KTH
Sommestad T., Franke U. A test of intrusion alert filtering based on network information. Security and Communication Networks, vol. 8:13, 2015.	FOI
Sommestad T., Hallberg J. A review of the theory of planned behaviour in the context of information security policy compliance. IFIP Advances in Information and Communication Technology, Vol. 405, 2013.	FOI
Sommestad T., Hallberg J., Lundholm K., Bengtsson J. Variables influencing information security policy compliance: A systematic review of quantitative studies. Information Management and Computer Security, vol. 22:1, 2014.	FOI
Sommestad T., Holm H. Alert verification through alert correlation—An empirical test of SnIPS. Information Security Journal, vol. 26:1, 2017.	FOI
Sommestad T., Hunstad A. Intrusion detection and the role of the system administrator. Information Management and Computer Security, vol. 21:1, 2013.	FOI
Sommestad T., Karlzén H., Hallberg J. A meta-Analysis of studies on protection motivation theory and information security behaviour. International Journal of Information Security and Privacy, vol. 9:1, 2015.	FOI

Sommestad T., Karlzén H., Hallberg J. The sufficiency of the theory of planned behavior for explaining information security policy compliance. Information and Computer Security, vol. 23:2, 2015.	FOI
Sommestad T., Karlzén H., Nilsson P., Hallberg J. An empirical test of the perceived relationship between risk and the constituents severity and probability. Information and Computer Security, vol. 24:2, 2016.	FOI
Sommestad T., Karlzén H., Nilsson P., Hallberg J. Perceived information security risk as a function of probability and severity. Proceedings of the 9th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2015, 2015.	FOI
Sommestad T., Sandström F. An empirical test of the accuracy of an attack graph analysis tool. Information and Computer Security, vol. 23:5, 2015.	FOI, Umeå
Sou K.C., Sandberg H., Johansson K.H. On the exact solution to a smart grid cyber-security analysis problem. IEEE Transactions on Smart Grid, vol. 4:2, 2013.	KTH
Spjuth O., Heikkinen J., Litton J.-E., Palmgren J., Krestyaninova M. Data integration between Swedish national clinical health registries and biobanks using an availability system. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8574 LNBI, 2014.	Karolinska
Stankovski P., Brynielsson L., Hell M. The efficiency of optimal sampling in the random S-box model. IEEE International Symposium on Information Theory - Proceedings, 2014.	Lund
Stankovski P., Hell M., Johansson T. An efficient state recovery attack on the X-FCSR family of stream ciphers. Journal of Cryptology, vol. 27:1, 2014.	Lund
Stark L., King J., Page X., Lampinen A., Vitak J., Wisniewski P., Whalen T., Good N. Bridging the gap between privacy by design and privacy in practice. Conference on Human Factors in Computing Systems - Proceedings, Vol. 07-12-May-2016, 2016.	Stockholm
Stefan D., Levy A., Russo A., Maziéres D. Building secure systems with LIO (demo). Haskell 2014 - Proceedings of the 2014 ACM SIGPLAN Haskell Symposium, 2014.	Chalmers
Steinhauer H.J., Karlsson A., Andler S.F. Traceable uncertainty for threat evaluation in air to ground scenarios. Proceedings of the 16th International Conference on Information Fusion, FUSION 2013, 2013.	Skövde
Stirparo P. A fuzzing framework for the security evaluation of NDEF message format. Proceedings - 5th International Conference on Computational Intelligence, Communication Systems, and Networks, CICSyN 2013, 2013.	KTH

Stirparo P., Fovino I.N., Taddeo M., Kounelis I. In-memory credentials robbery on android phones. 2013 World Congress on Internet Security, WorldCIS 2013, 2013.	KTH
Stokes K., Carlsson N. A peer-to-peer agent community for digital oblivion in online social networks. 2013 11th Annual Conference on Privacy, Security and Trust, PST 2013, 2013.	Linköping
Strandberg K., Olovsson T., Jonsson E. Securing the Connected Car: A Security-Enhancement Methodology. IEEE Vehicular Technology Magazine, vol. 13:1, 2018.	Chalmers
Strydis C., Seepers R.M., Peris-Lopez P., Siskos D., Sourdis I. A system architecture, processor, and communication protocol for secure implants. Transactions on Architecture and Code Optimization, vol. 10:4, 2013.	Chalmers
Stuckman J., Walden J., Scandariato R. The effect of dimensionality reduction on software vulnerability prediction models. IEEE Transactions on Reliability, vol. 66:1, 2017.	Chalmers, Göteborg
Sulaman S.M., Orucevic-Alagic A., Borg M., Wnuk K., Host M., De La Vara J.L. Development of safety-critical software systems using open source software- A systematic map. Proceedings - 40th Euromicro Conference Series on Software Engineering and Advanced Applications, SEAA 2014, 2014.	Lund
Sulaman S.M., Weyns K., Host M. Identification of IT Incidents for Improved Risk Analysis by Using Machine Learning. Proceedings - 41st Euromicro Conference on Software Engineering and Advanced Applications, SEAA 2015, 2015.	Lund
Sulaman S.M., Weyns K., Höst M. A review of research on risk analysis methods for IT systems. ACM International Conference Proceeding Series, 2013.	Lund
Sulaman S.M., Wnuk K., Höst M. Perspective based risk analysis-a controlled experiment. ACM International Conference Proceeding Series, 2014.	Lund
Svantesson D.J.B. Against 'Against data exceptionalism'. Masaryk University Journal of Law and Technology, vol. 10:2, 2016.	Stockholm
Svantesson D.J.B. The (uncertain) future of online data privacy. Masaryk University Journal of Law and Technology, vol. 9:1, 2015.	Stockholm
Söderberg H., Khalid J., Rayees M., Dahlman J., Falkmer T. In video war games, are military personnel's fixation patterns different compared with those of civilians?. Journal of Defense Modeling and Simulation, vol. 11:4, 2014.	Chalmers, Linköping
Søilen K.S., Nerme P., Stenström C., Darefelt N. Usage of internet banking among different segments as an example of innovation - trust	Halmstad

and information needs. Journal of Internet Banking and Commerce, vol. 18:2, 2013.	
Tahira S., Sher M., Ullah A., Imran M., Vasilakos A.V. Handover based IMS registration scheme for next generation mobile networks. Wireless Communications and Mobile Computing, Vol. 2017, 2017.	Luleå
Tan Z. An improved anonymous authentication scheme for roaming services. Journal of Information Hiding and Multimedia Signal Processing, vol. 6:2, 2015.	Uppsala
Tao S., Dubrova E. Reliable low-overhead arbiter-based physical unclonable functions for resource-constrained IoT devices. ACM International Conference Proceeding Series, 2017.	KTH
Tao S., Dubrova E. Temperature aware phase/frequency detector-basec RO-PUFs exploiting bulk-controlled oscillators. Proceedings of the 2017 Design, Automation and Test in Europe, DATE 2017, 2017.	KTH
Tao S., Dubrova E. TVL-TRNG: Sub-Microwatt True Random Number Generator Exploiting Metastability in Ternary Valued Latches. Proceedings of The International Symposium on Multiple-Valued Logic, 2017.	KTH
Tao S., Dubrova E. Ultra-energy-efficient temperature-stable physical unclonable function in 65 nm CMOS. Electronics Letters, vol. 52:10, 2016.	KTH
Tariq M.A., Brynielsson J., Artman H. The security awareness paradox: A case study. ASONAM 2014 - Proceedings of the 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, 2014.	FOI, KTH
Teixeira A., Shames I., Sandberg H., Johansson K.H. A secure control framework for resource-limited adversaries. Automatica, Vol. 51, 2015.	KTH
Teixeira A., Sou K.C., Sandberg H., Johansson K.H. Quantifying Cyber-Security for Networked Control Systems. Lecture Notes in Control and Information Sciences, Vol. 449 LNCIS, 2013.	Chalmers, KTH
Teljstedt C., Rosell M., Johansson F. A Semi-automatic Approach for Labeling Large Amounts of Automated and Non-automated Social Media User Accounts. Proceedings - 2nd European Network Intelligence Conference, ENIC 2015, 2015.	FOI, KTH
Thapa D., Harnesk D. Rethinking the information security risk practices: A critical social theory perspective. Proceedings of the Annual Hawaii International Conference on System Sciences, 2014.	Luleå
Tiger M., Heintz F. Towards unsupervised learning, classification and prediction of activities in a stream-based framework. Frontiers in Artificial Intelligence and Applications, Vol. 278, 2015.	Linköping

Tiloca M. Efficient protection of response messages in dtls-based secure multicast communication. ACM International Conference Proceeding Series, Vol. 2014-September, 2014.	SICS
Tiloca M., De Guglielmo D., DIni G., Anastasi G., Das S.K. JAMMY: A Distributed and Dynamic Solution to Selective Jamming Attack in TDMA WSNs. IEEE Transactions on Dependable and Secure Computing, vol. 14:4, 2017.	SICS
Tiloca M., Nikitin K., Raza S. Axiom: DTLS-based secure IoT group communication. ACM Transactions on Embedded Computing Systems, vol. 16:3, 2017.	SICS
Tiloca M., Racciatti F., Dini G. Simulative evaluation of security attacks in networked critical infrastructures. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9338, 2015.	SICS
Toghian M., Morogan M.C. Suggesting a method to improve encryption key management in wireless sensor networks. Indian Journal of Science and Technology, vol. 8:19, 2015.	KTH, Stockholm
Torra V. A fuzzy microaggregation algorithm using fuzzy c-means. Frontiers in Artificial Intelligence and Applications, Vol. 277, 2015.	Skövde
Torra V., Navarro-Arribas G. Big data privacy and anonymization. IFIP Advances in Information and Communication Technology, Vol. 498, 2016.	Skövde
Torra V., Navarro-Arribas G. Integral privacy. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10052 LNCS, 2016.	Skövde
Torra V., Navarro-Arribas G., Sanchez-Charles D., Muntés-Mulero V. Provenance and privacy. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10571 LNAI, 2017.	Skövde
Torrisi N.M., Vuković O., Dán G., Hagdahl S. Peekaboo: A gray hole attack on encrypted SCADA communication using traffic analysis. 2014 IEEE International Conference on Smart Grid Communications, SmartGridComm 2014, 2015.	KTH
Trabalza D., Raza S., Voigt T. INDIGO: Secure CoAP for Smartphones: Enabling E2E Secure Communication in the 6IoT. Communications in Computer and Information Science, Vol. 366 CCIS, 2013.	SICS, Uppsala
Tragos E.Z., Angelakis V., Fragkiadakis A., Gundlegard D., Nechifor C.-S., Oikonomou G., Pohls H.C., Gavras A. Enabling reliable and secure IoT-based smart city applications. 2014 IEEE International Conference on	Linköping

Pervasive Computing and Communication Workshops, PERCOM WORKSHOPS 2014, 2014.	
Trang D., Johansson F., Rosell M. Evaluating Algorithms for Detection of Compromised Social Media User Accounts. Proceedings - 2nd European Network Intelligence Conference, ENIC 2015, 2015.	FOI, Uppsala
Tudor V., Almgren M., Papatriantafilou M. A study on data de-pseudonymization in the smart grid. Proceedings of the 8th European Workshop on System Security, EuroSec 2015, 2015.	Chalmers
Tudor V., Almgren M., Papatriantafilou M. Employing Private Data in AMI Applications: Short Term Load Forecasting Using Differentially Private Aggregated Data. Proceedings - 13th IEEE International Conference on Ubiquitous Intelligence and Computing, 13th IEEE International Conference on Advanced and Trusted Computing, 16th IEEE International Conference on Scalable Computing and Communications, IEEE International Conference on Cloud and Big Data Computing, IEEE International Conference on Internet of People and IEEE Smart World Congress and Workshops, UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld 2016, 2017.	Chalmers
Tudor V., Almgren M., Papatriantafilou M. Harnessing the unknown in Advanced Metering Infrastructure traffic. Proceedings of the ACM Symposium on Applied Computing, Vol. 13-17-April-2015, 2015.	Chalmers
Tuma K., Scandariato R., Widman M., Sandberg C. Towards security threats that matter. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 10683 LNCS, 2018.	Göteborg, Volvo
Udd R., Asplund M., Nadjm-Tehrani S., Kazemtabrizi M., Ekstedt M. Exploiting bro for intrusion detection in a SCADA system. CPSS 2016 - Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security, Co-located with Asia CCS 2016, 2016.	KTH, Linköping
Ul Islam R., Hossain M.S., Andersson K. A novel anomaly detection algorithm for sensor data under uncertainty. Soft Computing, vol. 22:5, 2018.	Luleå
Ul Islam R., Schmidt M., Kolbe H.-J., Andersson K. Secure and scalable multimedia sharing between smart homes. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol. 5:3, 2014.	Luleå
Uppman U., Nilsson J., Sterner U. Jamming effects on multicast traffic in ad hoc networks for different terrains. Proceedings - IEEE Military Communications Conference MILCOM, 2016.	FOI
Ur Rahman M.M., Yasmeen A., Gross J. PHY layer authentication via drifting oscillators. 2014 IEEE Global Communications Conference, GLOBECOM 2014, 2014.	KTH

Urbina D.I., Giraldo J., Cardenas A.A., Tippenhauer N.O., Valente J., Faisal M., Ruths J., Candell R., Sandberg H. Limiting the impact of stealthy attacks on Industrial Control Systems. Proceedings of the ACM Conference on Computer and Communications Security, Vol. 24-28-October-2016, 2016.	KTH
Vahidi A. The Monotonic Separation Kernel. Proceedings - 2014 International Conference on Embedded and Ubiquitous Computing, EUC 2014, 2014.	SICS
Vahidi A., Jämthagen C. Secure RPC in embedded systems: Evaluation of some GlobalPlatform implementation alternatives. Proceedings of the Workshop on Embedded Systems Security, WESS 2013, 2013.	Lund, SICS
Valentini R., Levorato M., Fischione C. Performance analysis of IEEE 802.15.3c-Based mmW wireless networks. 2015 49th Annual Conference on Information Sciences and Systems, CISS 2015, 2015.	KTH
Valja M., Korman M., Shahzad K., Johnson P. Integrated metamodel for security analysis. Proceedings of the Annual Hawaii International Conference on System Sciences, Vol. 2015-March, 2015.	KTH
Wallgren L., Raza S., Voigt T. Routing attacks and countermeasures in the RPL-based internet of things. International Journal of Distributed Sensor Networks, Vol. 2013, 2013.	SICS, Uppsala
Van Acker S., Hausknecht D., Joosen W., Sabelfeld A. Password meters and generators on the web: From large-scale empirical study to getting it right. CODASPY 2015 - Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, 2015.	Chalmers
Van Acker S., Hausknecht D., Sabelfeld A. Data exfiltration in the face of CSP. ASIA CCS 2016 - Proceedings of the 11th ACM Asia Conference on Computer and Communications Security, 2016.	Chalmers
Van Acker S., Hausknecht D., Sabelfeld A. Measuring login webpage security. Proceedings of the ACM Symposium on Applied Computing, Vol. Part F128005, 2017.	Chalmers
Van Delft B., Broberg N., Sands D. A Datalog semantics for Paralocks. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 7783 LNCS, 2013.	Chalmers
Van Den Berghe A., Yskout K., Joosen W., Scandariato R. A model for provably secure software design. Proceedings - 2017 IEEE/ACM 5th International FME Workshop on Formal Methods in Software Engineering, FormaliSE 2017, 2017.	Göteborg
van den Berghe A., Scandariato R., Yskout K., Joosen W. Design notations for secure software: a systematic literature review. Software and Systems Modeling, vol. 16:3, 2017.	Göteborg

Wang H., Hell M., Johansson T., Ågren M. Improved key recovery attack on the BEAN stream cipher. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E96-A:6, 2013.	Lund
Wang Q., Skoglund M. Symmetric private information retrieval for MDS coded distributed storage. IEEE International Conference on Communications, 2017.	KTH
Wang S., Bi J., Wu J., Vasilakos A.V. CPHR: In-Network Caching for Information-Centric Networking with Partitioning and Hash-Routing. IEEE/ACM Transactions on Networking, vol. 24:5, 2016.	Luleå
Wang Y., Dai W., Zhang B., Ma J., Vasilakos A.V. Word of Mouth Mobile Crowdsourcing: Increasing Awareness of Physical, Cyber, and Social Interactions. IEEE Multimedia, vol. 24:4, 2017.	Luleå
Wang Y., Min Q., Han S. Understanding the effects of trust and risk on individual behavior toward social media platforms: A meta-analysis of the empirical evidence. Computers in Human Behavior, Vol. 56, 2016.	Stockholm
Wang Z., Xiao M., Skoglund M., Poor H.V. Secrecy degrees of freedom of wireless X networks using artificial noise alignment. IEEE International Symposium on Information Theory - Proceedings, Vol. 2015-June, 2015.	KTH
Vapen A., Carlsson N., Mahanti A., Shahmehri N. A look at the third-party identity management landscape. IEEE Internet Computing, vol. 20:2, 2016.	Linköping
Vapen A., Carlsson N., Mahanti A., Shahmehri N. Information sharing and user privacy in the third-party identity management landscape. CODASPY 2015 - Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, 2015.	Linköping
Varagnolo D., Pillonetto G., Schenato L. Distributed cardinality estimation in anonymous networks. IEEE Transactions on Automatic Control, vol. 59:3, 2014.	KTH
Vasilevskaya M., Gunawan L.A., Nadjm-Tehrani S., Herrmann P. Integrating security mechanisms into embedded systems by domain-specific modelling. Security and Communication Networks, vol. 7:12, 2014.	Linköping
Vasilevskaya M., Nadjm-Tehrani S. Model-based security risk analysis for networked embedded systems. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8985, 2016.	Linköping
Vasilevskaya M., Nadjm-Tehrani S. Quantifying risks to data assets using formal metrics in embedded system design. Lecture Notes in	Linköping

Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9337, 2015.	
Vaske C., Wecksten M., Jarpe E. Velody-A novel method for music steganography. 2017 3rd International Conference on Frontiers of Signal Processing, ICFSP 2017, 2017.	Halmstad
Vassena M., Breitner J., Russo A. Securing Concurrent Lazy Programs Against Information Leakage. Proceedings - IEEE Computer Security Foundations Symposium, 2017.	Chalmers
Vassena M., Buiras P., Waye L., Russo A. Flexible manipulation of labeled values for information-flow control libraries. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9878 LNCS, 2016.	Chalmers
Waye L., Buiras P., Arden O., Russo A., Chong S. Cryptographically secure information flow control on key-value stores. Proceedings of the ACM Conference on Computer and Communications Security, Vol. Part F131467, 2017.	Chalmers
Wazid M., Das A.K., Khan M.K., Al-Ghaiheb A.A.-D., Kumar N., Vasilakos A.V. Secure Authentication Scheme for Medicine Anti-Counterfeiting System in IoT Environment. IEEE Internet of Things Journal, vol. 4:5, 2017.	Luleå
Wearing T., Dragoni N. Security and privacy issues in health monitoring systems: Ecare@home case study. Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, Vol. 187, 2016.	Örebro
Weeraddana P.C., Fischione C. On the Privacy of Optimization. IFAC-PapersOnLine, vol. 50:1, 2017.	KTH
Wei Y., Wang L., Svensson T. Analysis of secrecy rate against eavesdroppers in MIMO modulation systems. 2015 International Conference on Wireless Communications and Signal Processing, WCSP 2015, 2015.	Chalmers
Wen F., Wang Z. Distributed Kalman filtering for robust state estimation over wireless sensor networks under malicious cyber attacks. Digital Signal Processing: A Review Journal, Vol. 78, 2018.	Chalmers
Wen L., Jiang W., Jiang K., Zhang X., Pan X., Zhou K. Detecting fault injection attacks on embedded real-time applications: A system-level perspective. Proceedings - 2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security and 2015 IEEE 12th International Conference on Embedded Software and Systems, HPCC-CSS-ICESS 2015, 2015.	Linköping
Verginadis Y., Michalas A., Gouvas P., Schiefer G., Hübsch G., Paraskakis I. PaaSword: A holistic data privacy and security by design framework	SICS

for cloud services. CLOSER 2015 - 5th International Conference on Cloud Computing and Services Science, Proceedings, 2015.	
Vernotte A., Johnson P., Ekstedt M., Lagerstrom R. In-depth modeling of the UNIX operating system for architectural cyber security analysis. Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOCW, Vol. 2017-October, 2017.	KTH
Westerlund M. Talking suicide: Online conversations about a taboo subject. Nordicom Review, vol. 34:2, 2013.	Karolinska
Westling A., Brynielsson J., Gustavi T. Mining the web for sympathy: The pussy riot case. Proceedings - 2014 IEEE Joint Intelligence and Security Informatics Conference, JISIC 2014, 2014.	FOI
Westphal F., Axelsson S., Neuhaus C., Polze A. VMI-PL: A monitoring language for virtual platforms using virtual machine introspection. Digital Investigation, vol. 11:SUPPL. 2, 2014.	Blekinge
Weyns K., Host M. Service level agreements in Municipal IT dependability management. Proceedings - International Conference on Research Challenges in Information Science, 2013.	Lund
Wiklund M., Mozelius P., Westin T., Norberg L. Biometric belt and braces for authentication in distance education. Proceedings of the European Conference on e-Learning, ECEL, Vol. 2016-January, 2016.	Stockholm
Wikström D. Simplified universal composability framework. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9562, 2016.	KTH
Winter P., Köwer R., Mulazzani M., Huber M., Schrittwieser S., Lindskog S., Weippl E. Spoiled onions: Exposing malicious Tor exit relays. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8555 LNCS, 2014.	Karlstad
Winter P., Pulls T., Fuss J. ScrambleSuit: A polymorphic network protocol to circumvent censorship. Proceedings of the ACM Conference on Computer and Communications Security, 2013.	Karlstad
Vitak J., Wisniewski P., Page X., Lampinen A., Litt E., De Wolf R., Kelley P.G., Sleeper M. The future of networked privacy: Challenges and opportunities. Proceedings of the ACM Conference on Computer Supported Cooperative Work, CSCW, Vol. 2015-January, 2015.	Stockholm
Volkamer M., Renaud K., Canova G., Reinheimer B., Braun K. Design and field evaluation of PassSec: Raising and sustaining web surfer risk awareness. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9229, 2015.	Karlstad

Volkamer M., Renaud K., Reinheimer B., Kunz A. User experiences of TORPEDO: TOoltip-poweRed Phishing Email DetectiOn. Computers and Security, Vol. 71, 2017.	Karlstad
Woltjer R. Workarounds and trade-offs in information security-An exploratory study. Information and Computer Security, vol. 25:4, 2017.	FOI
Voronkov A., Iwaya L.H., Martucci L.A., Lindskog S. Systematic literature review on usability of firewall configuration. ACM Computing Surveys, vol. 50:6, 2017.	Karlstad
Voronkov A., Lindskog S., Martucci L.A. Challenges in Managing Firewalls. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9417, 2015.	Karlstad
Wu S., Guo Z., Shi D., Johansson K.H., Shi L. Optimal innovation-based deception attack on remote state estimation. Proceedings of the American Control Conference, 2017.	KTH
Wu Y., Xiao Y., Hohn F., Nordstrom L., Wang J., Zhao W. Bad Data Detection Using Linear WLS and Sampled Values in Digital Substations. IEEE Transactions on Power Delivery, vol. 33:1, 2018.	KTH
Vuković O., Dán G. On the security of distributed power system state estimation under targeted attacks. Proceedings of the ACM Symposium on Applied Computing, 2013.	KTH
Vukovic O., Dan G. Security of fully distributed power system state estimation: Detection and mitigation of data integrity attacks. IEEE Journal on Selected Areas in Communications, vol. 32:7, 2014.	KTH
Vuković O., Dán G., Bobba R.B. Confidentiality-preserving obfuscation for cloud-based power system contingency analysis. 2013 IEEE International Conference on Smart Grid Communications, SmartGridComm 2013, 2013.	KTH
Välja M., Korman M., Lagerström R. A study on software vulnerabilities and weaknesses of embedded systems in power networks. Proceedings - 2017 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, CPSR-SG 2017 (part of CPS Week), 2017.	KTH
Wästerfors D., Burcar1 V. Safety work with an ethnic slant. Social Inclusion, vol. 2:3, 2014.	Lund
Xia Z., Xiong N.N., Vasilakos A.V., Sun X. EPCBIR: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing. Information Sciences, Vol. 387, 2017.	Luleå
Xu C., Wedlund D., Helgoson M., Risch T. Model-based validation of streaming data. DEBS 2013 - Proceedings of the 7th ACM International Conference on Distributed Event-Based Systems, 2013.	Uppsala

Yalew S.D., Maguire G.Q., Haridi S., Correia M. T2Droid: A trustzone-based dynamic analyser for android applications. Proceedings - 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 11th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Conference on Embedded Software and Systems, Trustcom/BigDataSE/ICESS 2017, 2017.	KTH
Yalew S.D., Maguire G.Q., Jr., Correia M. Light-SPD: A platform to prototype secure mobile applications. PAMCO 2016 - Proceedings of the 2nd MobiHoc International Workshop on Privacy-Aware Mobile Computing, 2016.	KTH
Yan Z., Ding W., Niemi V., Vasilakos A.V. Two Schemes of Privacy-Preserving Trust Evaluation. Future Generation Computer Systems, Vol. 62, 2016.	Luleå
Yan Z., Li X., Wang M., Vasilakos A.V. Flexible Data Access Control Based on Trust and Reputation in Cloud Computing. IEEE Transactions on Cloud Computing, vol. 5:3, 2017.	Luleå
Yan Z., Wang M., Li Y., Vasilakos A.V. Encrypted Data Management with Deduplication in Cloud Computing. IEEE Cloud Computing, vol. 3:2, 2016.	Luleå
Yano E.T., Bhatt P., Gustavsson P.M., Ahlfeldt R.-M. Towards a methodology for cybersecurity risk management using agents paradigm. Proceedings - 2014 IEEE Joint Intelligence and Security Informatics Conference, JISIC 2014, 2014.	Skövde
Yu X., Yan Z., Vasilakos A.V. A Survey of Verifiable Computation. Mobile Networks and Applications, vol. 22:3, 2017.	Luleå
Yu Y., Xue L., Au M.H., Susilo W., Ni J., Zhang Y., Vasilakos A.V., Shen J. Cloud data integrity checking with an identity-based auditing mechanism from RSA. Future Generation Computer Systems, Vol. 62, 2016.	Luleå
Zalasiński M., Cpałka K., Rakus-Andersson E. An idea of the dynamic signature verification based on a hybrid approach. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 9693, 2016.	Blekinge
Zec M., Kajtazi M. Examining how IT professionals in SMEs take decisions about implementing cyber security strategy. Proceedings of the European Conference on IS Management and Evaluation, ECIME, Vol. 2015-January, 2015.	Linné, Örebro
Zhang G., Fischer-Hubner S. Counteract DNS attacks on SIP proxies using bloom filters. Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013, 2013.	Karlstad

Zhang J., Hou R., Fan J., Liu K., Zhang L., McKee S.A. RAGuard: A hardware based mechanism for backward-edge control-flow integrity. ACM International Conference on Computing Frontiers 2017, CF 2017, 2017.	Chalmers
Zhang K., Papadimitratos P. GNSS receiver tracking performance analysis under distance-decreasing attacks. Proceedings of 2015 International Conference on Localization and GNSS, ICL-GNSS 2015, 2015.	KTH
Zhang S., Yu L., Wakefield R.L., Leidner D.E. Friend or foe: Cyberbullying in social network sites. Data Base for Advances in Information Systems, vol. 47:1, 2016.	Lund
Zhang W., Li X., Xiong N., Vasilakos A.V. Android platform-based individual privacy information protection system. Personal and Ubiquitous Computing, vol. 20:6, 2016.	Luleå
Zhang X., Zhan J., Jiang W., Ma Y., Jiang K. Design optimization of energy-And security-critical distributed real-time embedded systems. Proceedings - IEEE 27th International Parallel and Distributed Processing Symposium Workshops and PhD Forum, IPDPSW 2013, 2013.	Linköping
Zhao F., Luo H., Zhao X., Pang Z., Park H. HYFI: Hybrid Floor Identification Based on Wireless Fingerprinting and Barometric Pressure. IEEE Transactions on Industrial Informatics, vol. 13:1, 2017.	ABB
Zhao H., Kallander W., Johnson H., Wu S.F. SmartWiki: A reliable and conflict-refrained Wiki model based on reader differentiation and social context analysis. Knowledge-Based Systems, Vol. 47, 2013.	Blekinge
Zhong Y., Sullivan J., Li H. Face attribute prediction using off-the-shelf CNN features. 2016 International Conference on Biometrics, ICB 2016, 2016.	KTH
Åhlfeldt R.-M., Huvala I. Patient Safety and Patient Privacy When Patient Reading Their Medical Records. Communications in Computer and Information Science, Vol. 450 CCIS, 2014.	Skövde
Östberg K., Törngren M., Asplund F., Bengtsson M. Intelligent transport systems - The role of a safety loop for holistic safety management. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), Vol. 8696 LNCS, 2014.	Chalmers

FOI är en huvudsakligen uppdragsfinansierad myndighet under Försvarsdepartementet. Kärnverksamheten är forskning, metod- och teknikutveckling till nytta för försvar och säkerhet. Organisationen har cirka 1000 anställda varav ungefär 800 är forskare. Detta gör organisationen till Sveriges största forskningsinstitut. FOI ger kunderna tillgång till ledande expertis inom ett stort antal tillämpningsområden såsom säkerhetspolitiska studier och analyser inom försvar och säkerhet, bedömning av olika typer av hot, system för ledning och hantering av kriser, skydd mot och hantering av farliga ämnen, IT-säkerhet och nya sensorers möjligheter.

FOI
Totalförsvarets forskningsinstitut
164 90 Stockholm

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

www.foi.se