Security in Industrial Control Systems

Nationellt Centrum för säkerhet i styrsystem för samhällsviktig verksamhet (NCS3) är ett kompetenscentrum med uppdraget att bygga upp och sprida medvetenhet, kunskap och erfarenhet om cybersäkerhetsasspekter inom industriella informations- och styrsystem. Centrumets är ett samarbete mellan de svenska myndigheterna FOI och MSB och dess verksamhet fokuserar på aktörer som äger och/eller driver samhällsviktig verksamhet där industriella informations- och styrsystem ingår.

The National Centre for increased security in industrial control systems is a centre of excellence focused at building and disseminating awareness, knowledge and experience about cyber security aspects in ICS. The Centre is a cooperation between the Swedish Defence Research Agency and the Swedish Civil Contingencies Agency and the activities is focused on actors that owns and/or operates critical infrastructure where ICS are a part.

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Phone +46 8 555 030 00
Fax +46 8 555 031 00

www.foi.se

Swedish Civil Contingencies Agency
SE-651 81 Karlstad

Phone: +46 (0) 771-240 240
Fax: +46 (0) 10-240 56 00

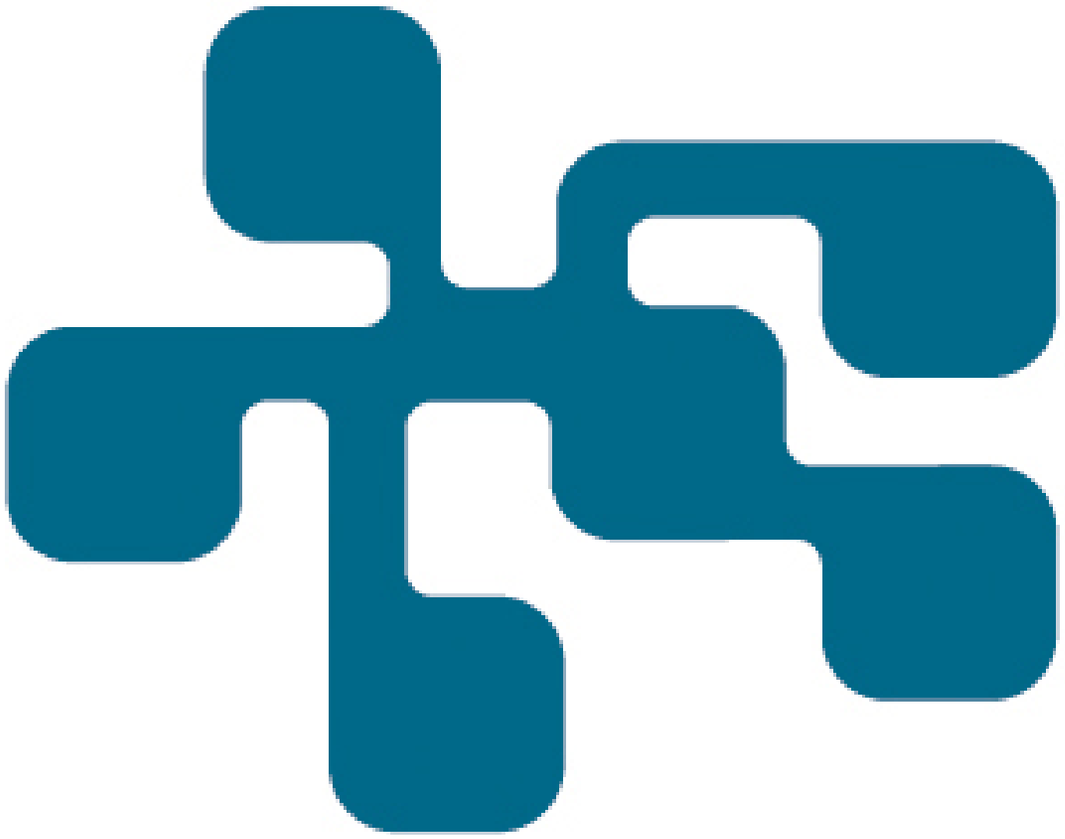
www.msb.se

Monitorerings- och övervakningssystem

En kategorisering och översikt av IDS-teknik inom IIS

AMUND GUDMUNDSON HUNSTAD, MARTIN KARRESAND

FOI
MSB



FOI-R--4420--SE
MSB 2014-1131
ISSN 1650-1942

April 2017

Amund Gudmundson Hunstad
Martin Karresand

Monitorerings- och övervakningssystem

En kategorisering och översikt av IDS-teknik inom IIS

Titel	Monitorerings- och övervakningssystem – En kategorisering och översikt inom IIS
Title	Monitoring and policing systems – A categorization and survey within ICS
Rapportnr/Report no	FOI-R--4420--SE
Månad/Month	april
Utgivningsår/Year	2017
Antal sidor/Pages	38
ISSN	1650-1942
Kund/Customer	MSB
Forskningsområde	4. Informationssäkerhet och kommunikation
FoT-område	Välj ett objekt.
Projektnr/Project no	E72097
Godkänd av/Approved by	Christian Jönsson
Ansvarig avdelning	Ledningssystem

Sammanfattning

Rapporten presenterar ett ramverk för klassificering av intrångsdetekteringssystem (IDS) för industriella informations- och styrsystem (IIS) baserat på existerande ramverk för IDS för IT-system. Ramverket kan till exempel användas som underlag vid behovsanalys, kravställning och anskaffning av IDS för IIS. Vidare ges i rapporten exempel på befintlig forskning och kommersiella system inom området. I rapporten konstateras att IIS medför ett antal specifika krav på förmågor hos IDS och att IIS IT-säkerhetsmässigt ligger efter i utvecklingen relativt den ökade internetuppkopplingen av system som pågår. Behovet av fungerande och anpassade IDS för IIS är därför stort.

Nyckelord: IDS, intrångsdetektering, industriella styrsystem, SCADA, IT-säkerhet

Summary

The report presents a frame work for classification of intrusion detection systems (IDS) used in Industrial Control Systems (ICS) based on existing frame works for IDS in IT systems. The frame work can function as a support when performing requirements engineering and procurement of IDS for ICS. Furthermore the report gives examples of current research and commercial systems within the area. The report shows that IDS for ICS are subject to a number of specific requirements and that ICS IT security wise is under-developed in relative to the increasing internet connection of such systems. The need for working and adapted IDS for ICS is therefore significant.

Keywords:IDS, intrusion detection, industrial control system, SCADA, IT security

Innehållsförteckning

1 Inledning

Ett industriellt informations- och styrsystem (IIS) består till stora delar av specialkomponenter som är robusta och driftsäkra och specialanpassade. Det utför repetitiva och väldefinierade uppgifter i form av mätning och styrning av processer inom infrastruktur av olika slag. Länge har dylika system varit fysiskt separerade från övriga IT-system och framför allt internet, men har under senare år i allt högre grad kopplats ihop med kontorssystem och internet för att förenkla och sänka kostnaderna för administration, styrning och övervakning på distans. De ingående komponenterna har traditionellt aldrig behövt vara skyddade mot IT-angrepp, vilket i kombination med lång livslängd hos utrustning i befintliga installationer gör att systemen är dåligt skyddade mot antagonistiska hot. Detta är särskilt olyckligt i och med en ökad exponering mot internet. En grundläggande skyddsfunktion för IT-system är användning av intrångsdetekteringssystem (IDS), som automatiskt ska upptäcka misstänkt aktivitet och intrångsförsök i det system som övervakas.

1.1 Bakgrund

MSB bedriver verksamhet för att öka medvetenheten kring behovet av skydd av IIS. De tar även fram råd och rekommendationer för hur skyddet av dylika system bör se ut. I råden ingår rekommendationer om användning av intrångsdetekteringssystem (IDS) som en del i skyddsåtgärderna (sid. 48–49, MSB, 2014; MSB, 2009). MSB har därför som en del i arbetet för säkrare IIS beställt en studie av IDS för IIS.

Begreppet ”intrusion detection system” för IT-system introducerades av Dorothy Denning (1987) och har sedan dess vuxit till ett omfattande område med ett flertal kommersiella produkter och en solid bas av forskning. De hittillsvarande systemen är dock främst framtagna för IT-system utan koppling till styrning och övervakning av industriella processer (fortsättningsvis kallade IT-system). De tar därför inte hänsyn de speciella krav som ett IIS ställer på dem. Samtidigt kan argumenteras för att båda systemtyperna bygger på samma koncept och att de delar som är värda att angripa till stora delar utgörs av vanlig IT-hårdvara och mjukvara, vilket skulle göra att kommersiella IDS-produkter går att använda även för ett IIS efter viss modifiering. Dock saknas exempelvis till stor del signaturer för IIS-specifika angrepp.

1.2 Syfte och avgränsningar

Studien syftar bland annat till att erbjuda ett underlag för fördjupning och uppdatering av MSB:s råd gällande användning av IDS för IIS. Som ett led i detta tas ett ramverk för kategorisering av IDS för IIS fram, baserat på

existerande ramverk för IDS för IT-system. Ramverket är tänkt att kunna fungera som stöd vid införskaffande av IDS för IIS, men främst i tidigare stadier av processen där en översikt av de tekniska möjligheter som erbjuds inom IDS-området är till nytta. Arbetet har en övergripande och framåtblickande karaktär och fokuserar inte på enstaka produkter.

1.3 Målgrupp

Den primära målgruppen för rapporten är systemägare av IIS som funderar på eller planerar att införskaffa IDS för att skydda systemet. Även annan verksamhet inom IIS-området kan ha användning för rapporten som en översikt av IDS-området och de parametrar som styr dylika systems funktion på en övergripande nivå.

1.4 Speciella IIS-krav

De krav som IIS ställer på IDS specificeras bland annat av Mitchell (2014) och Zhu (2014). Skillnaderna mellan IT-system och ett IIS beror främst på den ofta specialiserade hårdvaran i IIS och den tätare kopplingen till fysiska parametrar hos IIS. Det finns även högre krav på tillgänglighet och tidsrelevans[1] i och med att IIS ofta utgör hårda realtidssystem. Likaså har den processnära hårdvaran ofta begränsad mängd minne och beräkningskraft jämfört med vad IT-system har enligt Stouffer (2015). Det gör att ett IDS för IT-system inte kan användas utan modfiering, vilket gör att viktiga delar av ett IIS därför är sämre skyddade genom att angrepp mot dem inte kan upptäckas lika lätt. Ett flertal forskare beskriver ett antal skillnader mellan de båda systemtyperna ur en IDS-synvinkel (Mitchell, 2014; Zhu, 2014; Stouffer, 2015; Oman och Phillips, 2008).

- Den kanske mest uppenbara skillnaden mellan IT-system och IIS är de senares krav på realtidsförmåga. Styrningen av en övervakad process tillåter inte fördröjningar. När en instruktion behöver utföras måste den direkt få tillgång till processorn. I ett vanligt IT-system är det inte ovanligt att uppgifter som inte har med direkt användarinteraktion att göra läggs i en kö och utförs i turordning utan direkta krav på när de utförs. Det gör också att det inte finns några specifika krav på hur lång tid processorn kan vara upptagen. Att kombinera dessa två koncept är därför svårt, eftersom en instruktion med realtidskrav kan fördröjas under obestämd tid av en icke tidskritisk instruktion. I ett IDS-perspektiv innebär detta att de befintliga sensorer och detekteringsfunktioner som används är svåra eller omöjliga att införa i

[1] Det engelska uttrycket ”timeliness” kan översättas till tidsrelevans om innebörden är att ”aktuella data finns tillhands när de behövs, dvs. information har aktualitet” [Terminologicentrum, 2017].

IIS-system, eftersom de kan förorsaka att systemet inte uppfyller realtidskraven.

- I IT-system övervakar en IDS vad som händer i nätverk och på enskilda värddatorer. Det handlar då om händelser i den logiska domänen i de operativsystem och program som körs på datorerna. Där styrs händelserna inte av fysiska lagar vilket gör att det är svårt att uttala sig om sannolikheten för olika händelsekedjor. Dessutom kan antalet möjliga händelser vara mycket stort. Därför kan de händelser som inträffar i IT-system variera mycket och vara svåra att kategorisera på ett tydligt sätt. I IIS övervakar en IDS även händelser som styrs av de fysikaliska lagarna, vilket gör att vissa händelser lätt kan bedömas vara mindre sannolika än andra och övervakningen därför blir lättare. Det kan exempelvis handla om att vätskor i rörledningar rör sig från högre till lägre punkter om de inte pumpas och att flödet förbi en ventil minskar när den stängs och inte tvärt om. Även det faktum att IIS har ett väl definierat och avgränsat användningsområde bidrar till en mindre mängd möjliga användningsfall och därmed gör det lättare att övervaka med hjälp av ett IDS.
- I IIS är många funktioner automatiserade och bygger på slutna loopar där förändringar i styrningen återkopplas genom att fysiska mätvärden ändras. Det gör att beteendet blir repetitivt och förutsägbart på ett helt annat sätt än i IT-system där användarnas agerande medför en osäkerhetsfaktor som ökar antalet möjliga utfall och i praktiken ger vad som kan framstå som ett slumpmässigt beteende hos systemet. Ur ett intrångsdetekteringsperspektiv är det därför lättare att hantera IIS.
- IIS har generellt sett sämre (eller helt saknar eftersom det inte har varit ett krav) autentiseringsmekanismer än IT-system (Oman och Phillips, 2008). Det är också viktigt att separationen mellan administrativa nät och processnät är tillräcklig, annars kan autentisering och rättigheter i ett nät spilla över i ett annat. Dessa saker försvårar intrångsdetektering genom att det är svårt att skilja mellan legitima och avvikande sessioner, vilket annars är ett fundament för intrångsdetektering. Det saknas dessutom ofta ordentlig rättighetshantering i de processnära delarna av IIS, vilket ytterligare försämrar möjligheterna att särskilja tillåten och otillåten aktivitet i systemet eftersom, något förenklat, de enda inställningsmöjligheterna är att alla får göra allt, eller ingen göra något.
- I och med att ett IIS kan påverka omgivningen rent fysiskt utgör dylika system angreppsmål med högre värde än IT-system, vars förstörelse visserligen kan förorsaka stor ekonomisk skada, men inte direkt medför fara för människor. Om ett IIS som styr till exempel ett vattenverk eller ett system för eldistribution kan fås att bete sig felaktigt kan miljontals människor i värsta fall påverkas. Det gör också att dess tillgänglighet

och tidsrelevans är helt avgörande. Om flera program körs samtidigt på en enhet ökar risken för systemkrascher genom buggar i och med det ökade antalet involverade kodrader, under förutsättning att de olika programmen har likartat fördelning av buggar i koden. Situationen kan mycket förenklat liknas vid att varje program motsvarar en vanlig tärning och att en etta motsvarar en bugg. Ju fler tärningar som slås desto större sannolikhet att minst en tärning visar en etta. För att hjälpligt motverka detta tillkortakommande kan IDS-funktionaliteten placeras externt i särskilt avsedd hårdvara på nätverksnivå, men det medför fortfarande vissa begränsningar av detekteringsförmågan i och med nätverkstrafiken inte säger så mycket om aktuell status på komponenterna.

- De centrala (processnära) komponenterna av IIS innehåller ofta tillverkarspecifika operativsystem och kretsar, vilket gör det svårare att byta ut dem om ett säkerhetshål upptäcks och behöver åtgärdas. Ett byte av en dylik komponent kräver sannolikt att nya regler för processtyrning måste konstrueras och det i en ny utvecklingsmiljö. Det medför därför också att eventuella IDS-parametrar måste ändras och testas även de. Detta faktum gör det svårt att kombinera kraven på driftsäkerhet med kraven på IT-säkerhetsuppdateringar och uppdatering av eventuella IDS-regler.
- De processnära delarna i ett IIS har begränsningar i beräkningskraft och minnesutrymme relativt vanlig IT-utrustning, vilket gör att de ofta inte klarar av att hantera den extra belastning ett IDS för IT-system utgör. Realtidskraven som ställs på IIS medför dessutom en större känslighet mot variationer i exekveringshastighet vilket inte fungerar bra ihop med det dynamiska beteendet hos ett IDS.
- De processnära delar i ett IIS är främst avsedda att vara robusta och tåliga mot fel, vilket i vissa fall kan innebära att de är extra osäkra ur ett intrångsperspektiv. Det ska vara lätt att få kontakt med dem och styra dem, något som försvåras vid användning av IT-säkerhetsfunktioner. Målet att de alltid ska fungera gör också att säkerhetsuppdatering av firmware, om sådan är möjlig, vid upptäckt av nya säkerhetshål kanske inte utförs eftersom risken för att processtyrningen påverkas negativt bedöms vara för hög. Det kan även medföra att IT-säkerhetsrelaterade grundinställningar (till exempel lösenord) inte ändras om det inte är nödvändigt ur driftsynpunkt.
- Realtidskrav på de processnära delarna i ett IIS och bristen på datalagringsutrymme gör att det ofta saknas loggning av händelser kopplade till inloggning. Det försvårar intrångsdetektering och analys av misstänkta intrångsförsök. Ett alternativ är att logga till en extern enhet, men det löser bara problemet med datalagringsutrymme.

1.5 Läsanvisningar

Avsnitt 2 presenterar och förklarar det ramverk som tagits fram för kategorisering av IDS i IIS. När så behövs används exempel för att förtydliga och underlätta förståelsen för de principer som ligger bakom det som presenteras. I avsnitt 3 redovisas ett urval artiklar med inriktning mot intrångsdetektering i IIS för att visa på huvuddragen i den forsknings som pågår inom området. Avsnitt 4 innehåller en redovisning av några kommersiella system och marknadsaktörers syn på området. I avsnitt 5 diskuteras slutligen de resultat som framkommit i studien.

2 Klassificeringsramverk

Det ramverk för klassificering av IDS för IIS som har tagits fram är baserat på existerande ramverk för IDS för IT-system. De klassificeringsramverk (Abdulhammed, 2016; Bontupalli, 2016; Ganapathy, 2013; Liao, 2013; Milenkoski, 2015; Mitchell, 2014; Nazer, 2011; Poston, 2013; Vasilomanolakis, 2015) som hittats och bedömts relevanta är mycket lika på en grundläggande nivå, viss terminologi kan skilja, men de bakomliggande egenskaperna hos intrångsdetekteringssystem generellt är desamma. De konceptuella likheterna mellan IDS för IT-system och IDS för IIS är stor, vilket gör att det framtagna ramverket fungerar för båda varianterna av IDS. En förklaring till detta är att de kriterier som ingår ligger på en så pass hög abstraktionsnivå att de skillnader som finns mellan IT-system och IIS inte slår igenom. Det är även så att begränsningen i beräkningskraft och kravet på realtidsfunktion hos de processnära delarna av IIS gör att de delarna än så länge inte utrustas med IDS-funktionalitet i någon nämnvärd omfattning. Kvar blir de administrativa delarna (kontorsnät) av IIS och de är i grund och botten desamma som i IT-system, vilket gör att vanliga IDS kan användas med endast konfigurationsanpassningar.

Utvecklingen inom IDS-området har visat på ett behov av olika slags arkitekturer för intrångsdetekteringssystem. Behovet har uppkommit på grund av utvecklingen av korrelering[2] av larm från flera olika intrångsdetekteringssystem. Denna teknik kan liknas vid en över-IDS, som använder andra intrångsdetekteringssystem som sensorer, vilka i sin tur är fullt fungerande intrångsdetekteringssystem med egna sensorer. Tillsammans utgör de ett system-av-system. En dylik över-IDS har en *distribuerad* arkitektur. Termen kan kännas udda, men är vald för att även omfatta vanliga intrångsdetekteringssystem som består av flera samverkande fullvärdiga system. Den mest framträdande funktionen hos en distribuerade IDS är det faktum att delar av analys och detektering sker utspritt i det system eller nätverk som ska övervakas. Det tillför en ökad komplexitet och ökar angreppsmöjligheterna på själva intrångsdetekteringssystemet jämfört med ett IDS för *centraliserad* arkitektur, främst genom angrepp på kommunikationen mellan de ingående systemen. Den positiva effekten är en ökad detekteringsförmåga vad gäller avancerade och samverkande angrepp, samt till viss mån en ökad robusthet i och med att delar av en under-IDS kan falla ifrån utan att det överliggande intrångsdetekteringssystemet stannar. Detekteringsprestandan kan dock påverkas negativt, på samma sätt som om delar av sensorerna faller bort för en centraliserad IDS.

[2] Korrelering innebär att likhet mellan olika signaler, i IDS-fallet sekvenser av intrångslarm från olika intrångsdetekteringssystem, jämförs och mäts.

Tillsammans med arkitektur finns det ytterligare två kategorier som utgör grunden för i stort sett alla klassificeringsramverk för intrångsdetekteringssystem och de är typen av detektor och typen av datakälla. Detektorer delas in i kategorierna *signaturbaserad* och *anomalibaserad*. Det förekommer även hybridkategorier i vissa klassificeringar på grund av att de IDS som studerats innehåller båda typerna av detektorer. En signaturbaserad detektor använder förutbestämda mönster (signaturer) för att identifiera intrång. Principen bygger på att alla aktiviteter antas vara ofarliga, förutom de som matchar en signatur. Vid anomalibaserad detektering är det istället avvikelser i användningsmönster som ligger i fokus. IDS tränas på att känna igen mönster för hur systemet används och betraktar sedan avvikande aktiviteter som möjliga intrångsförsök.

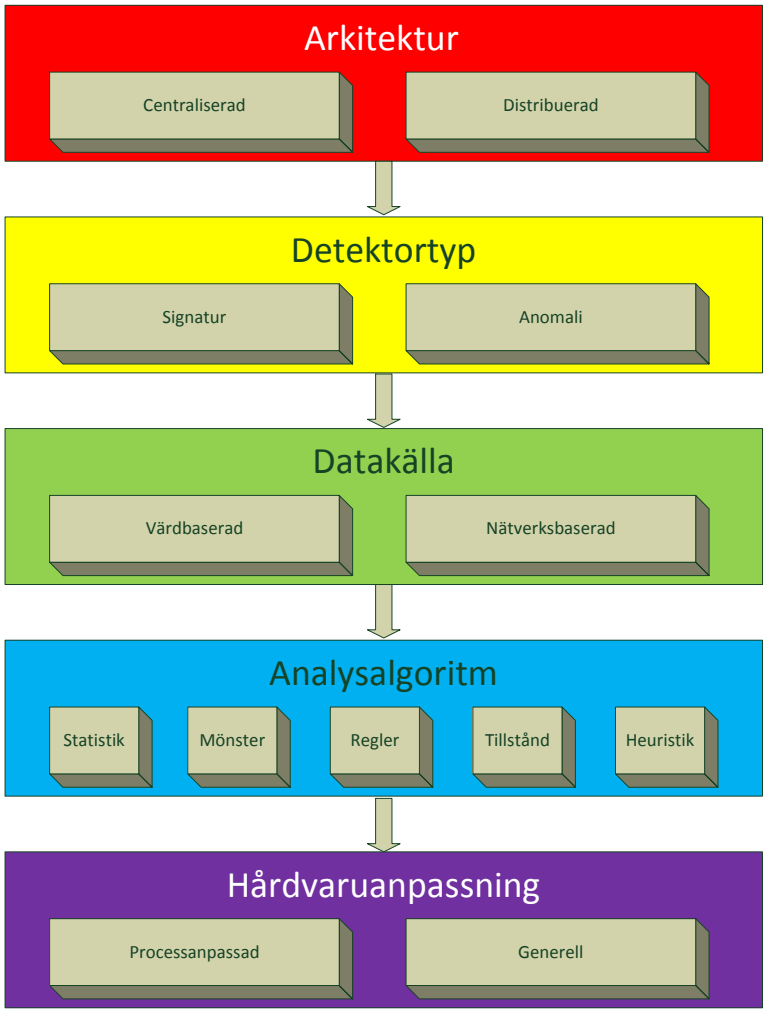
Kategorin datakälla delas in i kategorierna *värdbaserad* och *nätverksbaserad*. Det är dock inte ovanligt att andra termer används för de olika kategorierna, funktionen är dock densamma i grund och botten. Värdbaserad datainsamling sker på den enhet där sensorerna sitter och dataunderlaget utgörs främst av loggar och andra systemtillstånd. Nätverksbaserad datainsamling sker som namnet antyder i nätverk och utgörs av trafikinformation och nätverkspaket. Denna typ av insamling sköts ofta av en dedikerad hårdvara och via speciella portar i nätverksutrusningen.

En ofta använd kategori för klassificering av IDS är den typ av analysalgoritm som används för att omvandla sensordata från datakällan till faktiska larm. De olika typerna av analysalgoritmer är delvis knutna till typen av detektor, men det finns inte något absolut beroende mellan dem. Vissa algoritmer passar bättre ihop med signaturbaserad detektering och andra med anomalidetekterande. Till exempel passar exakta mönstermatchande algoritmer bra i signaturbaserade intrångsdetekteringssystem medan självlärande approximativa algoritmer passar bättre i anomalibaserade system. Det är dock ingenting som förhindrar att algoritmerna används tillsammans med valfri detektortyp, detekteringsförmågan kan dock bli lidande.

Analysalgoritmerna är under ständig utveckling, det är algoritmens effektivitet med avseende på korrekt detektering av angrepp som avgör hur bra en IDS presterar. Bra prestanda innebär hög andel korrekta larm tillsammans med en låg andel falsklarm. Algoritmutvecklingen hämtar inspiration från en rad områden och expanderar ständigt. De främsta bidragsgivarna finns inom artificiell intelligens, statistisk mönsterigenkänning och data mining. Denna kategori fylls ständigt på med nya algoritmtyper och kan därför komma att ändras i framtiden. Valet av typer har dock gjorts för att de i möjligaste mån ska vara heltäckande och tillräckligt generella för att stå sig även i framtiden.

I och med att intrångsdetekteringssystem har blivit aktuellt att använda även i IIS uppstår ett behov av en kategori i det framtagna ramverket som tar hänsyn till eventuell anpassning av ett IDS så att det kan verka tillsammans med processnära hårdvara och inte bara i IT-system.

I figur 1 visas hur de fem kategorierna i klassificeringsramverket hänger ihop. De tre övre kategorierna, arkitektur, detektortyp och datakälla utgör grunden för ramverket med de viktigaste kategorierna, vilka också ligger till grund för traditionell IDS-klassificering. De två nedre kategorierna är forskningsnära och förekommer inte alltid i andra klassificeringsramverk. Kategorin för analysalgoritm är heltäckande genom användning av klassen heuristik och kan komma att utökas eller förändras i och med att nya forskningsområden tillkommer. Bland annat kan heuristikklassen komma att delas upp i flera delar där en eventuell ny klass är artificiell intelligens. Längst ner kommer kategorin för anpassning för processnära hårdvara, vilken även den kan komma att delas upp i flera klasser när nya forsknings- och tillämpningsområden tar form.



Figur 1 Ramverk för IDS-klassificering. De tre övre kategorierna utgör grunden för traditionell IDS-klassificering. De två nedre kategorierna är mer forskningsnära och kan komma att förändras.

Vi anskaffning av IDS för IIS bör systemägaren ställa sig ett antal frågor med det framtagna ramverket som grund. Svaren på frågorna är beroende av systemägarens kännedom om systemet vilket underlättas av en uppdaterad risk- och sårbarhetsanalys.

- Vilka punkter i systemet har direkt eller indirekt kontakt med internet?
- Vilka delar i systemet utgör nyckelfunktioner med extra behörighet att modifiera och styra systemet?

- Hur pass förutsägbart beteende har systemet?
- Kan systemet, helt eller delvis, hantera att eventuella realtidskrav frångås?
- Hur homogent är systemet, det vill säga är det väl sammanhållet och enhetligt byggt (fysiskt och logiskt), eller är det distribuerat och består av flera generationer utrustning?

Beroende på svaren på frågorna passar olika alternativ i det framtagna ramverket bättre. Dessa utgör en vägledning i valet av lämplig IDS-modell.

2.1 Arkitektur

Ett IDS kan ha antingen en *centraliserad* eller *distribuerad* arkitektur. De första systemen för intrångsdetektering var centraliserade, men i takt med att storleken och komplexiteten på de system som skulle skyddas ökade skiftade fokus inom forskningen till distribuerad intrångsdetektering. Detta berode även på trenden att i ökad grad använda globala webb- och molntjänster. Numera är de system som intrångsdetekteringssystem installeras i distribuerade, vilket gör det naturligt att även det skyddande systemet övergår till att vara distribuerat.

2.1.1 Centraliserad intrångsdetektering

Centraliserad intrångsdetektering utgörs av en samling sensorer utan egen analysförmåga eller intelligens, som alla rapporterar till en central analysserver. Alla beslut, och därmed även beslut om larm, tas av den centrala servern, vilket gör den till en nyckeltjänst, som om den blir framgångsrikt angripen medför att hela intrångsdetekteringssystemet slås ut. Å andra sidan är den centrala servern lättare att skydda i och med att den körs på en enskild hårdvara, som dessutom kan vara utformad med redundans. Det är således bara en punkt som behöver skyddas och den behöver bara ha dedikerade kopplingar till sensorerna för att fungera.

2.1.2 Distribuerad intrångsdetektering

I begreppet distribuerad intrångsdetektering återfinns både komplexa lösningar med system-av-system av intrångsdetekteringssystem som rapporterar till varandra och tillsammans (eventuellt med en huvudaktör) analyserar och upptäcker intrång. Begreppet rymmer även system med intelligenta sensorer, även om ett dylikt i sig inte nödvändigtvis utgör ett fullvärdigt IDS. Korrelering av larm har länge varit populärt inom IDS-området och bland de vetenskapliga bidrag med inriktning mot intrångsdetekteringssystem för IIS som studerats har

ett flertal någon slags korreleringsfunktion och är därmed distribuerade (Vasilomanolakis, 2015).

2.2 Detektortyp

De två kategorier av detektorer som utgör grunden i de flesta klassificeringsramverk för IDS, *signaturbaserad* och *anomalibaserad*, skiljer sig åt vad gäller sättet att modellera systemet de övervakar.

2.2.1 Signaturbaserad intrångsdetektering

En signaturbaserad detektor bygger på modellering av angrepp. Principen kallas i vissa artiklar för *kunskapsbaserad detektering, felanvändningsdetektering* eller *svartlistning*. Termen kunskapsbaserad detektering kommer från det faktum att det är befintlig kunskap om hur intrång går till och vilka spår de lämnar som ligger till grund för framtagningen av signaturerna. Termen felanvändning kommer naturligt ur föregående term, det är felanvändning av systemet som ska detekteras och som signaturerna beskriver. Svartlistning är en term som förekommer inom många områden, till exempel sportevenemang, där personer som klassats som huliganer är svartlistade och därför inte får komma in på matcharenor. Alla som inte är svartlistade är dock välkomna. Inom IDS-området innebär svartlistning att signaturerna utgör en lista med förbjudna åtgärder i ett system, åtgärder som ska upptäckas och förhindras.

De signaturer som utgör grunden i detektorn är signaturer av kända angrepp, vilka därmed måste uppdateras för att hållas aktuella. Principen med modellering av angrepp gör att all annan trafik klassificeras som tillåten, något som passar bra i system med mycket och snabb variation av beteendet över tid (hög dynamik). Om aktiviteten i systemet är svår att förutsäga och har låg autokorrelation (inga tydliga mönster) är ett sätt att hålla nere falsklarm att inrikta detekteringen på att känna igen tecken på (kända) intrång. Det medför dock att hittills okända intrångstekniker inte detekteras och risken för falska negativ (riktiga intrång som klassas som ofarliga) inte ska försummas.

Det faktum att de signaturer som används kontinuerligt måste uppdateras gör att underhållet av en signaturbaserad detektor är resurskrävande. Uppdatering av IDS-databasen med signaturer, särskilt om systemet är distribuerad, innebär ett omfattande arbetsmoment. En ännu större arbetsinsats måste dock läggas på att underhålla, uppdatera och utöka antalet signaturer. Tecken på nya intrångsvarianter måste upptäckas, analyseras och omvandlas till signaturer med tillräckligt hög precision för att hålla falsklarmen nere utan att detekteringsgraden blir lidande. Därför erbjuds ofta uppdateringar i form av en prenumeration, där IDS-leverantören står för arbetet med att ta fram nya uppdateringar och sedan på olika sätt distribuerar signaturerna till systemet.

Framtagning av nya signaturer kan till viss del automatiseras, men bör inbegripa manuell kontroll för att inte fel ska smyga sig in, det vill säga att otillåtna beteenden klassas som tillåtna.

2.2.2 Anomalibaserad intrångsdetektering

Anomalidetektering bygger på modellering av normaltillstånd hos system och kallas även för *beteendebaserad detektering* eller *vitlistning*. Beteendebaserad detektering beskriver principen för vad detektorer styrs av. Genom att modellera normalbeteende och betrakta alla avvikelser (anomalier) som potentiella intrång kan även nya, hittills okända angrepp upptäckas. Det krävs dock att normalbeteendet är relativt regelbundet och lätt att avgränsa. Termen vitlistning är motsatsen till svartlistning. Vitlistning tillämpas exempelvis vid evenemang där bara personer som är bjudna är välkomna att delta. Termen motsvarar inom IDS-området att endast de beteenden och händelser som systemet tränats att känna igen är tillåtna i det övervakade systemet.

Det vanligaste sättet att skapa en modell för normalbeteendet hos ett system är att ha en IDS-träningsfas innan systemet börjar användas skarpt. Under träningsfasen samlar intrångsdetekteringssystemet in data från sina sensorer och lär sig vad som är ett normalt beteende hos det övervakade systemet. I och med att sättet att använda ett system förändras över tid på grund av systemuppdateringar, förändrade rutiner, byte av personal med mera, behöver dock modellen av normalbeteendet för systemet också förändras. En vanlig lösning är att låta detektorn till viss del vara självlärande och på så sätt automatiskt hålla sig i fas med det förändrade beteendemönstret. Det finns dock flera nackdelar med en sådan lösning. För det första kan en målmedveten angripare som har tid på sig långsamt vänja systemet vid en attack och på så sätt till slut få intrångsdetekteringssystemet att acceptera angriparens aktivitet i det övervakade systemet. Likaså kan snabba beteendeförändringar, till exempel vid större omorganisationer, ge upphov till en stor mängd falsklarm innan systemet lärt om. Det gör också att larm om riktigt angrepp lätt försvinner bland alla falsklarm. De operatörer som är satta att övervaka IDS-larm missar helt enkelt de skarpa larmen, eller så stänger de helt eller delvis av larmfunktionen tills det övervakade systemets nya användningsprofil har stabiliserats. Detta kan dessutom innebära en öppning för nya angrepp i och med att systemet inte klarar av att larma korrekt. Otillåtet beteende kan av systemet råka betraktas som tillåtet under tiden det lär sig det nya beteendemönstret.

En modell för beteendet hos det övervakade systemet kan även skapas i förväg utan att någon träningsfas genom att till exempel ett nätverksprotokoll används som bas. Konceptet liknar i det fallet arbetet med att framställa signaturer, men i och med att det är tillåten trafik som modelleras faller det under anomalidetektering. Detta gör att systemet har ett mycket väl avgränsat område för vad som är ett godtagbart beteende. På så vis kombineras fördelarna med

signaturer (tydlig definition) och anomalidetektering (hantering av hittills okända angrepp). En nackdel är dock att angrepp som bygger på fel i den bakomliggande standarden inte detekteras. De kommer att accepteras av intrångsdetekteringssystemet på samma sätt som vid träning på ett system där en angripare redan är inne och kan generera trafik som framstår som legitim. Likaså fungerar metoden sämre på enkla protokoll, till exempel Modbus där nyttolastdelens innehåll utgör en viktig attackvektor, eftersom protokollstandarder sällan noggrant specificerar datainnehåll. Även om det tas fram regler även för nyttolastdelen av paketen är det svårt, vilket i praktiken innebär att en stor del av paketinnehållet därför inte kommer att användas för detektering fullt ut.

2.3 Datakälla

De datakällor som används för kategorisering av IDS-teknik är *värddator* och *nätverk*. Begreppet värddator ska ses som komplementet till nätverk, det vill säga allt som inte är nätverkstrafik är värddatorbaserad datainsamling. Ursprungligen var huvuddelen av intrångsdetekteringssystemen värddatorbaserade. Dennings (1987) artikel, som drar upp riktlinjerna för IDS, är mycket värddatorcentrerad. Av de åtta exempel på tecken på intrång som listas är sju värddatorrelaterat. Denna datakälla kan därför ses som den ursprungliga datakällan. Detta har dock förändrats över tid och numera sker mycket av intrångsdetekteringen baserat på nätverkstrafik.

2.3.1 Värdbaserad datainsamling

Värddatorbaserad datainsamling innebär att de data som ligger till grund för intrångsdetekteringen samlas in lokalt i den aktuella hårdvaran. Det vill säga det som samlas in är på något sätt relaterat till tillståndet hos hårdvaran. Det kan vara kommandon som skickas till processorn, pekare och data i RAM, dekrypterad och bearbetad nätverkstrafik och loggfiler med (system)händelser.

En nackdel med värdbaserad datainsamling är att eventuella tecken på intrång detekteras senare än för nätverksbaserad datainsamling. Till exempel har ett angrepp med skadlig kod nått närmare operativsystemets kärna och processorn om det detekteras inne i systemet, än om det detekteras redan på nätverksnivå.

En fördel med värdbaserad datainsamling är att värddatorns eller -systemets beteende kan övervakas mer i detalj än vid nätverksbaserad datainsamling. Detta eftersom eventuell skadlig kod som skickats över nätverket har mottagits i sin helhet och aktiverats, vilket ger fler och tydligare tecken på att systemet är angripet. Det gör att hittills okända angrepp lättare kan detekteras via värdbaserad datainsamling än via nätverksbaserad.

Värdbaserad datainsamling är också det enda realistiska alternativet vid end-to-endkrypterad nätverkstrafik i och med att den nätverkstrafik som går mellan noderna i nätverket är krypterad med nycklar som endast de inblandade noderna har tillgång till. En värdbaserad IDS kan genom sin placering få tillgång till data efter att de dekrypterats och på så sätt upptäcka attacker. Det gör att en värdbaserad IDS inte behöver ha tillgång till några kryptonycklar för att utföra sitt arbete.

2.3.2 Nätverksbaserad datainsamling

Nätverksbaserad datainsamling innebär att data som skickas över nätverk samlas in under transport, företrädelsevis i nätverksutrustning (switchar, brandväggar med mera). Ett nätverkspaket består av två delar, ett huvud med information om paketet, ungefär motsvarande adressetiketten på ett fysiskt paket, och en del med nyttolast, det vill säga de data som transporteras. Om mycket data ska överföras kommer de att hackas upp i mindre bitar (fragmenteras) och skickas i flera paket, som sedan sätts ihop av mottagaren. Detta motsvarar en leverans med flera kollin i den fysiska världen.

Till skillnad från värdbaserad datainsamling är den skadliga koden på nätverksnivå bara en bit data i mängden av data som transporteras i nätverket och kan då lättare fås att se ofarlig ut. Likaså medför fragmenterade nätverkspaket att ett paket eventuellt bara innehåller delar av alla tecken som behövs för att upptäcka ett angrepp. Dock kan angrepp som använder fel och brister i nätverksprotokoll genom att använda ge felaktig information i pakethuvudet detekteras vid nätverksbaserad datainsamling (detta är vanligt vid förberedelser för kommande intrång och vid överbelastningsattacker), likaså medför insamlingspunkten att angrepp kan upptäckas tidigare än vid värdbaserad datainsamling.

Nätverksbaserad data utgör data från hela nätverkspaket, det vill säga både nyttolasten och de metadata som flaggorna i pakethuvudet utgör. Nätverksbaserad datainsamling görs oftast med hjälp av dedikerad hårdvara, för det mesta i samband med brandväggsfunktioner. Insamlingen kan ske både på ut- och insidan av en brandvägg. De två sätten har olika för- och nackdelar.

Insamling på utsidan av en brandvägg medför en ofiltrerad datamängd, där alla angreppsförsök som riktas mot systemet kommer med. Det innebär en större belastning för analysdelen i ett IDS än vid insamling innanför brandväggen. Å andra sidan ger det en bättre bild av den aktuella hotbilden mot systemet än vid insamling på insidan.

Insamling på insidan av en brandvägg ger en datamängd som filtrerats av brandväggen och som därmed bara innehåller angreppsförsök som inte brandväggen kunnat skydda mot. Om brandväggen fungerar väl innebär det därför en lägre belastning på analysdelen av intrångsdetekteringssystemet än vid

datainsamling på utsidan. Dessa angrepp har dock penetrerat brandväggen och kravet på korrekt detektering är därför högt.

Om möjligt bör nätverksbaserad insamling ske både på ut- och insidan av en brandvägg för att dra nytta av fördelarna från båda koncepten. Det kan dock kräva en dubblering av IDS-funktionen beroende på hur det aktuella intrångsdetekteringssystemet är konfigurerat.

Till skillnad från en värdbaserad IDS måste en nätverksbaserad IDS ha tillgång till de kryptonycklar som används vid end-to-endkrypterad nätverkstrafik för att kunna hantera nyttolastpaketdelen av nätverkspaket. Om ett IDS ges tillgång till nycklarna medför det att det skydd som end-to-endkrypteringen skulle ge försvagas eller till och med elimineras. Att ge ett nätverksbaserat IDS tillgång till kryptonycklar som skyddar kommunikationen i ett system gör dessutom intrångsdetekteringssystemet till ett mycket hett mål för en angripare. Ett nätverksbaserat IDS kan därför i praktiken bara läsa nätverkspaketens metadata, det vill säga pakethuvuden, övriga data är och bör vara krypterade.

2.4 Analysalgoritm

Det är inom området analysalgoritmer som den mesta forskningen kring IDS bedrivs. Aktiviteten är konstant hög med cirka 1250 artiklar per år i medeltal de senaste 10 åren enligt Holm och Sommestad (2016). Områdets utveckling gör att intresset för olika delområden varierar och därmed också antalet publikationer inom dem. Sedan millennieskiftet har artiklar skrivits inom en mängd delområden. I en artikel av Liao m fl från (2013) har 30 forskningsartiklar från 22 delområden sammanställts och kategoriserats. Sammanställning ligger till grund för den ramverkskategori som berör analysalgoritmer. De 22 delområdena har dock delvis slagits samman för att generalisera ramverkskategorin och på så sätt göra den stabilare över tid och därmed mer användbar. De kategorier som det framtagna ramverket innehåller är *statistikbaserade, mönsterbaserade, regelbaserade, tillståndsbaserade* och *heuristikbaserade*.

Eftersom utvecklingshastigheten inom de olika algoritmområdena växlar går det inte att gradera någon kategori som mer aktuell än någon annan. Statistik- respektive mönsterbaserade algoritmer verkar vara de vanligast förekommande algoritmerna i dagsläget, detta baseras dock endast på rapportförfattarnas uppfattning efter att arbetet med insamling av bakgrundsmaterialet var klart. Antalet artiklar som klassificerats av Liao m fl inom respektive algoritmtyp redovisas i samband med beskrivningen av respektive typ. Vissa artiklar ingår dock i flera kategorier, så summan av artiklar överstiger 30.

2.4.1 Statistikbaserade algoritmer

Att använda statistiska mätmetoder för att skilja mellan olika typer av system- och nätverksaktiviteter är vanligt inom IDS-området. Det kan handla om generella statistiska mått med inriktning mot gruppering och klassificering, men även mer specialiserade algoritmer används. Det kan då till exempel handla om att mäta avstånd mellan en förlaga och en misstänkt onormal händelse, beräkna sannolikheten för en händelse givet vissa kända omständigheter, eller använda spelteori för att bestämma en trolig väg fram till en viss händelse och på så sätt se om den är onormal. De algoritmer och matematiska principer som används omfattar bland annat metoder för att jämföra medel- och medianvärden, hur mycket en fördelning av data varierar och om fördelningen för en viss typ av data alltid är sned, det vill säga att det alltid förekommer mer av en viss typ data än en annan.

Exempel: Om en dörr övervakas kontrolleras att den öppnas och stängs ungefär lika många gånger varje dag och att de flesta öppningar och stängningar sker dagtid beräknat över ett dygn. Om avvikelsen blir för stor kommer algoritmen att skicka ut ett larm.

Liao et al redovisar 17 vetenskapliga artiklar inom området.

2.4.2 Mönsterbaserade algoritmer

Mönsterbaserade algoritmer bygger på mönsterigenkänning, det vill säga olika sätt att jämföra sekvenser av händelser och data för att se hur lika de är. Området kan vid en första anblick verka tätt knutet till signaturbaserad detektering, men är minst lika relevant för att hitta anomalier.

Exempel: Om en dörr övervakas kontrollerar de mönsterbaserade algoritmerna till exempel att tiden för hur länge dörren är öppen respektive stängd stämmer överens med en mall för hur den brukar, eller ska, användas.

Förutom vanlig matchning av en misstänkt onormal händelse mot ett förbestämt mönster finns även algoritmer för jämförelse av fysisk interaktion med system, till exempel mönster för tangentbordsanvändning och vilka filer som användarna använder och modifierar. Sådana algoritmer kan anpassas för de processnära delarna av IIS. Även grafisk redovisning av händelsemönster har provats inom IDS-området för att hjälpa operatörer att manuellt avgöra om en händelse är ett misstänkt intrång eller inte.

Liao et al redovisar 8 vetenskapliga artiklar inom området.

2.4.3 Regelbaserade algoritmer

Regelbaserade algoritmer bygger som namnet antyder på ett specifikt framtaget regelverk för hur ett system ska uppföra sig. Till grund för regelverket kan ligga till exempel en specifikation av ett nätverksprotokoll. Specifikationen överförs till ett språk som ett IDS förstår och systemet kan sedan kontrollera att aktiviteter i det övervakade systemet inte bryter mot reglerna.

Exempel: Om en dörr övervakas kan reglerna säga att den får vara öppen, eller stängd och låst. Är dörren stängd men inte låst är det ett regelbrott och en intrångsvarning skickas.

Inom det regelbaserade algoritmområdet återfinns även tekniker för att sålla ut data ur stora datamängder, så kalla data mining, men även metoder för att skapa modeller av till exempel beteende. Det senare är en grundfunktion inom anomalidetektering.

Liao et al redovisar 16 vetenskapliga artiklar inom området.

2.4.4 Tillståndsbaserade algoritmer

De tillståndsbaserade algoritmerna bygger alla på logiskt sammankopplade lägen eller tillstånd för det övervakade systemet. Vid varje legitim händelse i systemet hamnar det i något av alla de tillstånd som är tillåtna för systemet. Förflyttningen mellan tillstånden får bara ske enligt förutbestämda vägar. Om en avvikande händelse inträffar försätts systemet i ett otillåtet tillstånd, det vill säga ett tillstånd som inte med i uppsättningen av godkända tillstånd. Principen liknar funktionen hos de regelbaserade algoritmerna, men fokuserar på hur tillståndet i systemet ska vara, inte vilka aktiviteter som är tillåtna. Med hjälp av till exempel programkoden för det system som ska övervakas skapas en logisk modell, ett träd, av alla möjliga vägar genom programkoden. Detta är dock bara praktiskt genomförbart för relativt små program, men passar bra med den logiska styrningen av de processnära delarna av IIS.

Exempel: Om en dörr övervakas får den vara öppen, stängd och olåst, eller stängd och låst. Att den är öppen och låst är ett otillåtet tillstånd och den kan heller inte förflytta sig direkt mellan tillståndet stängd och låst till öppen och låst utan att först ha passerat stängd och olåst.

Inom området finns även algoritmer som bygger på analys av till exempel nätverksprotokoll för att avgöra tillåtna och otillåtna tillstånd. Där ryms också algoritmer för bedömning av användarnas intentioner med olika beteenden.

Liao et al redovisar 13 vetenskapliga artiklar inom området.

2.4.5 Heuristikbaserade algoritmer

Ordet heuristik innebär en enkel procedur eller tumregel och härstammar från ett grekiskt ord som betyder *upptäcka*. Termen används ibland som en slaskkategori där sådant som inte går att klassificera i någon annan grupp hamnar. Vad gäller intrångsdetektering återfinns algoritmer som företrädelsevis har anknytning till artificiell intelligens och självlärande eller -utvecklande tekniker. Det kan till exempel handla om neurala nätverk som försöker efterlikna hur hjärnan är uppbyggd och fungerar, genetiska algoritmer som härmar den evolutionära utvecklingsprocessen, algoritmer som inspirerats av immunsystemet och beteendet hos fågel- och insektssvärmar, samt oskarp logik där uppsatta gränsvärden tillåts variera till viss del.

Exempel: Om en dörr övervakas lär sig heuristikbaserade algoritmer vad en dörr är, hur den ser ut och hur den fungerar, liksom hur den brukar användas och kan även på egen hand lära sig hur den bör och inte bör användas. Utifrån den kunskapen detekteras sedan felanvändning och ett av målen med sådana algoritmer är att överträffa förmågan till korrekt (intrångs)detektering hos mänskliga operatörer.

Liao et al redovisar 17 vetenskapliga artiklar inom området.

2.5 Hårdvaruanpassning

Utifrån det faktum att de processnära delarna av IIS ställer speciella krav på ett IDS har en kategori lagts till det framtagna ramverket för att särskilja ett specialanpassat IDS från IDS för IT-system. De alternativ som kategorin innehåller är *processanpassad* och *generell*. Kategorin avser de krav som presenteras i inledningen av rapporten, men i och med att IIS finns i en stor mängd radikalt olika miljöer och tillämpningar kan det dessutom finnas specialfall med ytterligare krav. Dessa specialfall får hanteras utanför det framtagna ramverket, alternativt föras in som en uppdatering av ramverket vid ett senare tillfälle.

2.5.1 Processanpassad intrångsdetektering

Alternativet processanpassad intrångsdetektering täcker de olika specialanpassade intrångsdetekteringssystem som övervakar styrningen av den fysiska delen av processen i ett IIS för att förhindra till exempel felinställda ventiler, vilka tillsammans kan förorsaka skada på utrustningen. Detta ger ett skydd mot angrepp via legitima instruktioner till den processnära hårdvaran, eventuellt under lång tid, som tillslut försätts i ett felaktigt tillstånd. Intrångsdetekteringssystem som tillhör detta kategorialternativ kan mycket väl vara standardiserade och inte anpassade för något specifikt system. Det räcker med att de läser av processtyrningsdata och agerar utifrån den.

2.5.2 Generell intrångsdetektering

Begreppet generell intrångsdetektering avser intrångsdetekteringssystem konstruerade enbart för IT-system där inte någon specialanpassning till den processnära hårdvaran gjorts. Det är med andra ord komplementet till alternativet processanpassad IDS.

3 Aktuell forskning

Aktuell forskning inom IDS redovisar betydande bredd och djup, vilket svårt låter sig sammanfattas kort. I detta kapitel redovisas en översikt över huvudinriktningar i IDS-forskningen och exempel på enskilda forskningssatsningar. Tyngdpunkten ligger på senare års forskning (2007 till 2016) och därmed framkommer också observationer av vad som kan utgöra forskningsmässiga trender.

Vad som utgör adekvata och relevanta forskningsresultat för operativ verksamhet är inte alltid uppenbart. Operativa behov är inte givet de samma faktorer som påverkar forskningsinriktning. Det är inte heller givet att goda forskningsresultat är de som snabbt låter sig implementeras i kommersiella system och produkter. Behov av processanpassad IDS för IIS-behov utgör ytterligare faktorer som påverkar vad som är adekvata och relevanta forskningsresultat.

3.1 Huvudinriktningar och trender inom IDS-forskning

Kategorierna i klassificeringsramverket enligt avsnitt 2 ger ett tolkningsraster avseende olika intrångsdetekteringssystem, vilket ger en utmärkt infallsvinkel till existerande forskningslitteratur. Liao m fl (2012) redovisar forskningsläget 2012 på ett tillgängligt och tydligt sätt baserad på en taxonomi av olika IDS-metoder. De pekar på att olika tekniker har sina respektive styrkor såväl som begränsningar, vilka är viktiga att väga in vid teknikval. Detta medför att valen inte är givna och enkla, utan kräver avvägningar mellan olika verksamhetsbehov relativt vad olika lösningar kan erbjuda. En stor utmaning är således att hitta rätt balans mellan detekteringsförmåga och systempåverkan. Exempelvis beskrivs signaturbaserade metoders relativa enkelhet vid implementering, förhållandevis låga behov av processorkraft och goda förmåga att detektera kända attacker, samtidigt som dessa metoder inte kan detektera okända attacker, där signaturer inte än existerar.

Liao m fl (2012) pekar även på några framtida utmaningar. Till exempel lyfts intrångsdetektering i trådlösa nätverk fram som viktig, men med tydliga utmaningar avseende säkerhet, kommunikation och systemförvaltning. Heuristiska metoder och parallell datahantering lyfts också fram som intressanta framtida utvecklingsområden, samtidigt som dessa ställer betydande krav på processorkraft vid realtidshantering av attacker. IDS-hantering i virtualiserade miljöer är också en trend att följa, då detta bland annat är av intresse i samband med molnbaserade lösningar. Huruvida detta är relevant för IDS i IIS-sammanhang torde vara en separat fråga att granska, eftersom molnlösningar i sig ger betydande säkerhetsutmaningar.

3.2 Exempel på forskning

2007 startade The International Federation for Information Processing Working Group (IFIP WG) 11.10 en konferens inriktad på skydd av kritisk infrastruktur. Konferensen heter The International Conference on Critical Infrastructure Protection (ICCIP). Varje år publiceras en bok med ett urval av de artiklar som presenterats vid konferensen. Ungefär en artikel av cirka 15 per år i boken har inriktning mot intrångsdetektering i IIS. Ett urval av dessa artiklar sammanfattas nedan, som en palett av exempel på IDS-forskning med relevans för IIS.

Oman och Phillips (2008) presenterar en IDS som ska övervaka händelser i SCADA-system. Händelserna är främst kopplade till inloggning och konfigurationsförändringar i RTU:er. Systemet verkar främst råda bot på eventuella brister i loggning hos de övervakade enheterna och artikeln beskriver inte systemet i sådan detalj att det går att placera in deras IDS i klassificeringsramverket fullt ut. Det är dock signaturbaserat och bygger på intrångsdetekteringssystemet Snort, och kopplingen till RTU:er gör att det är ett processanpassat system.

Svendsen och Wolthusen (2008) beskriver ett anomalidetekterande intrångsdetekteringssystem som bygger på statistiska analysmetoder, något de säger passar bra för SCADA-system. De attacker som de försöker detektera är fysiska attacker på rörsystem för transport och produktion av naturgas. Genom att detektera avvikelser mellan olika borrhål avseende vatteninnehåll kan de se om någon försöker angripa systemet. Systemet är ett processanpassat IDS.

Svendsen och Wolthusen (2009) skriver att signaturbaserad IDS inte passar i SCADA-system eftersom så stora felmarginaler måste inkluderas i och med att systemet interagerar med fysiska processer. De signaturer som ska avgöra om en händelse är en attack eller inte blir av den anledningen inte tillräckligt exakta för att fungera bra. Svendsen och Wolthusen rekommenderar därför användning av anomalidetektering och ger praktiska exempel från ett vattenkraftverk där vissa kritiska parametrar med fördel övervakas av IDS. Artikeln presenterar inte ett IDS i egentlig mening, men de praktiska exemplen pekar mot en processanpassning.

Rrushi och Kang (2009) påpekar betydelsen av kopplingen mellan den fysiska och digitala delen av IIS. Vad som är normalt beteende i den fysiska delen är välkänt enligt dem och det kan utnyttjas för att detektera intrång även i den digitala delen av systemen. Deras sätt att göra det på är att inspektera nätverkspaket som manipulerar variabler i de processnära delarna och utifrån hur dessa variabler påverkar processen kan de sedan avgöra om det är ett intrång eller inte. Deras system är nätverksbaserat, processanpassat och anomalidetekterande med statistiska analysalgoritmer.

Nai Fovino m fl (2010) argumenterar för att korrelerad nätverksbaserad detektering med fokus på legitim trafik, det vill säga IDS där vanlig trafik sammanställs för att hitta avvikelser, är den metod som är att rekommendera. De vill bort ifrån fokuseringen på att hitta elakartade beteenden i nätverkstrafiken och menar att risken är att mer utdragna angreppsförlopp då riskerar att missas, eftersom de använder fullt legitima instruktioner som i en lång sekvens utgör ett angrepp. Deras lösning är en distribuerad modell där en hierarki av intrångsdetekteringssystem tillsammans upptäcker intrång som bygger på sekvenser av tillåtna instruktioner. Systemet är nätverksbaserat generellt signaturdetekterande med tillståndsanalys.

Klump och Kwiatkowski (2010) föreslår att intrångsdetektering i elektriska distributionsnät bör utföras i form av dynamiska listor över misstänkta och otillåtna IP-adresser. De visar även hur listorna kan distribueras och kommunikationen mellan olika ingående parter säkras mot påverkan och avlyssning för att säkerställa att listorna inte manipuleras. Valet av svartlistning av IP-adresser gör att deras system kan klassificeras som signaturbaserat och generellt.

Reeves m fl (2011) har konstruerat en generell värddatorbaserad IDS med låg belastning på processorn för att möjliggöra installation i realtidssystem. Placeringen av det intrångsdetekterande systemet gör det dock känslig för samma slags angrepp det ska detektera. Intrångsdetekteringssystemet lär sig i det fallet vilka systemanrop som sker till processorn i normalfallet och detekterar anomalier, men det kräver att systemet inte är eller blir angripet före och under inlärningsfasen. Risken finns alltså att eventuell befintlig elakartad kod klassificeras som normal.

Deng och Shukla (2013) fokuserar på sammanställning av händelser i SCADA-system för att detektera intrång. Händelserna omfattar allt som kan användas för att övervaka, styra och manipulera systemet. Händelserna rapporteras till en central server som sammanställer dem och avgör om en sekvens av händelser utgör ett intrång eller inte. För analysen används en tillståndsbaserad algoritm och systemet i sig är processanpassat.

Alajlouni och Rao (2013) har studerat ett anomalidetekterande system som bygger på tillstånd och statistiska algoritmer. Det har testats mot en modell av ett system för dricksvattenförsörjning, där sensordata från processtyrningen används som bas, vilket gör det processanpassat.

Hurst m fl (2014) har studerat säkerhetslösningar för kritisk infrastruktur på en generell nivå och kom fram till att de krav som IIS ställer på ett intrångsdetekteringssystem tillsammans med begränsningar i enskilda lösningar gör att flera olika typer av intrångsdetekteringssystem behövs för att maximera skyddet. De propagerar för användning av sammanställande hothanteringssystem

(unified threat management), där flera olika skyddsmekanismer samverkar, en av dem är IDS.

Caselli m fl (2015) har studerat nätverkstrafik som innehåller Modbus, MMS och IEC104-protokollen för att se om det går att detektera sekvenser av instruktioner som leder fram till intrång. Deras arbete utför en förberedelse inför skapandet av ett IDS som kan detektera attacksekvenser och går därför inte att klassificera med hjälp av ramverket. Inriktningen mot sekvenser indikerar dock att det verkar bli ett signaturbaserat IDS.

Peng m fl (2015) har byggt ett generellt anomalidetekterande nätverksbaserat IDS med enkla statistikalgoritmer vars datakälla är en modell, ett fingeravtryck, av det normala trafikmönstret i ett system. Några av de parametrar som används är storlek på paket, tid mellan paket, riktning på flödet och längd på TCP-sessioner. Den trafik som används för att skapa ett fingeravtryck av ett specifikt system går mellan en operatör och till exempel en PLC.

4 Befintliga kommersiella system

I detta kapitel beskrivs aktuellt utvecklingsläge avseende existerande intrångsdetekteringssystem. Utvecklingsläget beskrivs med utgångspunkt i klassificeringsramverket i avsnitt 2 och dess terminologi. Enskilda lösningar och system granskas i huvudsak inte. Intentionen är primärt att ur ett klassificeringsramverksperspektiv åskådliggöra den allmänna kommersiella utvecklingen och dess utmaningar på IDS-området.

4.1 Kommersiella system ur ett ramverksperspektiv

Sen (2015) och Poston (2012) noterar att signaturbaserade intrångsdetekteringssystem är dominerande bland kommersiella system i och med att de är relativt effektiva. Respektive signatur beskriver en känd typ av intrång eller attack. Deras tydligaste nackdel är att de är beroende av att signaturerna är kända av intrångsdetekteringssystemet, vilket medför att de inte kan detektera nya intrång eller intrångsvarianter som inte har någon signatur. Vidare innebär detta även att uppdatering av signaturdatabaser är en central utmaning. I och med att betydande mängder nya intrång uppträder dagligt, krävs också automatisk generering av nya signaturer.

Nazer och Selvakumar (2011) observerar att de flesta kommersiella intrångsdetekteringssystem baserar sig på enskilda tekniker, även om ett större antal tekniker har utvecklats. Huruvida kombinationer av tekniker är välfungerande, lyfts inte som fråga. Likasom Sen (2015) noterar Nazer och Selvakumar (2011) att signaturbaserad IDS dominerar bland kommersiella system och ger två skäl för detta:

- Kunskapsbaserade tillvägagångssätt är lättare att implementera än regelbaserade, ty regelbaserade tekniker har en högre kostnad i termer av falsklarm.
- Hastighet, i form av snabba bedömningar, har högre prioritet än uttrycksfullhet. Därmed används signaturer i stället för till exempel regelbaserade intrångsdetekteringssystem.

Enligt Nazer och Selvakumar (2011) är kommersiella system baserade på äldre forskningsresultat inom intrångsdetektering. Vidare argumenterar de för att forskningsfokus senare har ändrats mot skydd av infrastrukturen istället för slutanvändarnas datorer. Med denna utveckling har, enligt Nazer och Selvakumar (2011), fokus ändrats mot nätverkssniffande lösningar. Inayat m fl (2015) ger en något annorlunda bild av situationen avseende kommersiella lösningar, i och med en observation av att de flesta IDS är nätverksbaserade. Denna observation kan

mycket väl vara präglad av en utgångspunkt från en utvecklingsnivå fyra år senare och därmed baserad på i allmänhet nyare resultat.

Dominansen av signaturbaserade intrångsdetekteringssystem kan tolkas som att en potential finns för kommersialisering av ytterligare forskningsresultat och också den forskning inom andra kategorier så som redovisad i klassificeringsramverket i avsnitt 2. En kompletterande tolkning, som är mera tillbakadragen i sin optimism, är att dessa ytterligare forskningsresultat respektive kategorier är tänkbart svårare att kommersialisera. Vid kommersialisering tillkommer därmed andra, mera operativa krav, som forskning i mindre grad begränsas av.

4.2 Marknadsaktörsperspektiv

Som en del i arbetet med denna rapport har en enkel avstämning genomförts med två svenska marknadsaktörer som levererar intrångsdetekteringslösningar för IIS. Avstämningen redovisar dessa marknadsaktörers perspektiv på vad som är specifikt för intrångsdetektering för IIS och har genomförts i form av telefonsamtal med Robin von Post hos Sectra respektive Erik Johansson hos Westermo. Intentionen med avstämningen har varit att inhämta exempel på hur marknadsaktörer tänker och agerar, utan krav på fullständig kartläggning.

Robin von Post säger att Sectra tillhandahåller intrångsdetektering som en tjänst, vilket indikerar att de inte säljer någon specifik IDS-produkt, utan snarare ett koncept. De poängterar dock att det är viktigt att en IDS inte påverkar det övervakade systemet negativt på något sätt. Varje installation är därför unik och IDS-lösningen måste skräddarsys för det specifika systemet, vilket till exempel uppnås genom att skaffa sig god verksamhetsinsikt.

Westermo lyfter fram de näst intill statiska informationsflöden som är karakteristiska för IIS-baserade miljöer. Detta innebär att vad som är att bedöma som avvikande och oönskade händelser är i allmänhet synnerligen enklare och klarare än i exempelvis en kontorsmiljö. Informationsflöden i dessa IIS-baserade miljöer beskrivs av Westermo som näst intill deterministiska och givna av kända protokoll med väldefinierade beteenden. Det blir därför av stor vikt att ha god kontroll över alla enheter i system, och att koppla detta till en väldokumenterad förändringsprocess med redovisning av vad som utgör förväntade och acceptabla händelser, oönskade händelser respektive ännu inte klassificerade händelser. Därigenom kan system och verksamhet enklare skyddas.

Marknadsaktörernas perspektiv på vad som karakteriserar kommersiella IDS i IIS-sammanhang kompletterar ramverkets bild som inhämtats via forskningslitteratur. Där litteraturen tenderar att mera fokusera på metodikdetaljer, algoritmval och liknande aspekter, lyfter marknadsaktörerna mera fram aspekter kring kundrelationer och vad som utgör typiska och

karakteristiska informationsflöden. Företag är också i allmänhet av konkurrensskäl försiktiga med att redovisa detaljer kring metodik- och algoritmval. Därmed förekom det mindre av diskussion kring ramverket och dess uppbyggnad från marknadsaktörernas perspektiv.

5 Diskussion och slutsatser

Generella IDS-lösningar kan bara användas i de delar av IIS som innehåller vanlig IT-utrustning. De delar som avviker är de processnära delarna där övergången till fysisk styrning sker. De ställer krav på robusthet och realtidsexekvering, samtidigt som de i mångt och mycket fortfarande är mer eller mindre oskyddade mot IT-relaterade hot. Ett IDS för de processnära delarna behöver därför uppfylla samma krav som för processnära IIS för att vara användbara och samtidigt ha en tillräckligt hög detekteringsförmåga.

Genom att installera ett IDS i de IT-system som stödjer processdelen i IIS erhålls ett skydd mot intrång från en stor mängd av den skadliga kod som finns på internet. Ett dylikt system bör dock kompletteras med ett IDS som är anpassad för detektering i de processnära delarna av systemet. Med ramverket som grund kan konstateras att arkitektur, detektortyp och datakälla är desamma för ett IDS för IT-system och IIS-anpassad IDS. De data som används för detektering skiljer sig dock åt genom den direkta fysiska kopplingen till processen och de krav det ställer i IIS. Slutligen kan befintliga intrångsdetekteringsalgoritmer för ett IDS anpassas för användning även i de processnära delarna.

En viktig sak att beakta är att IIS generellt har sämre autentiseringsmekanismer än IT-system. Dessutom är separationen i många fall undermålig mellan de processnära delarna och de administrativa delarna av IIS. Detta resulterar i att det är svårt att skilja mellan legitima och avvikande sessioner, vilket är ett fundament för intrångsdetektering. Detta gäller framför allt de processnära delarna av IIS, men även administrativa delar som kopplats till internet utan en ordentlig IT-säkerhetsmässig genomgång kan ha allvarliga säkerhetsbrister. Generellt ligger ofta IIS efter i utvecklingen IT-säkerhetsmässigt och en komplicerande faktor vid uppdateringar är att systemet inte får stå still eftersom den process det styr då också stannar.

Det ramverk som presenteras i rapporten är baserat på olika ramverk för traditionell IDS som presenterats i den vetenskapliga litteraturen. Grunden för ramverket är de fyra första kategorierna 1) arkitektur 2) detektortyp 3) datakälla och 4) analysalgoritm. Den sista kategorin 5) anpassning för processnära hårdvara är ny och speciellt ämnad för ett IDS för IIS, men det ingående alternativet generell gör att ramverket kan appliceras även på ett IDS för IT-system.

Ramverket är tänkt att ge en bättre förståelse för hur ett IDS är uppbyggt och vilken funktionalitet som är viktig. På så sätt underlättas kravställning och övriga delar av anskaffningsprocessen för ett IDS genom att olika alternativ lättare kan jämföras. De tekniker som ligger bakom de olika kategorierna i ramverket har alla både för- och nackdelar och valet av lösning bör därför ske utifrån en noggrann analys av varje unikt system och situation. På forskningssidan, och till

viss del även kommersiellt, är trenden att sätta samman flera olika typer av skydd till en väl fungerande enhet, där varje del ansvarar för ett delområde i skyddet. Även om dylika system ger fler möjligheter för en angripare att skada och manipulera själva intrångsdetekteringssystemet, ökar även robustheten och förmågan till självövervakning, vilket ger en positiv övervikt åt systemets förmåga att ge ett fullgott skydd.

Kommersiell IDS-utveckling präglas av en del liknande utvecklingstendenser och trender som inom forskningsvärlden, men där kommersiella drivkrafter och kundbehov medför att ett annat urval av påverkansfaktorer är tongivande i och med att fokus inom den kommersiella världen ligger på att sälja vad som fungerar här och nu. Vad som är forskningsmässigt intressant är inte alltid kommersiellt gångbart eller ens möjligt att implementera i nuvarande system. I kommersiell verksamhet är också andra faktorer av vikt att väga in, så som en välutvecklad kundrelation baserad på över tid upparbetad tilltro och tillhandahållande av kvalitativa tjänster. Intrångsdetektering i IIS-sammanhang underlättas dessutom av nära statiska informationsflöden.

I MSB:s vägledning till ökad säkerhet i industriella informations- och styrsystem ges i punkt 9 rådet att kontinuerligt övervaka ett IIS för att upptäcka tecken på intrång [sid. 48–49, MSB, 2014]. Det är viktigt, men lika viktigt är att övervaka rätt delar. Mycket förenklat består IIS av en administrativ del där övervakning, styrning och loggning sker, ofta i form av programvara som körs på standarddatorer. Sedan finns den egentliga processtyrningen i form av de processnära delarna (PLC, RTU, m.m.). För att uppnå ett fullgott skydd bör alla delar i ett IIS övervakas av ett IDS. Att uppnå detta kan dock vara kostsamt, både rent ekonomiskt, men även i form av påverkan på systemet. Det behöver nödvändigtvis inte vara ett och samma system som hanterar de olika delarna i ett IIS. Om flera olika intrångsdetekteringssystem installeras bör de dock samarbeta på något sätt för att kunna ge en helhetsbild av de angrepp det övervakade systemet utsätts för.

Lämpligt val och korrekt placering av IDS kräver god kunskap om det system som ska skyddas. En kartläggning, till exempel i form av en risk- och sårbarhetsanalys, av systemet som ska övervakas är att rekommendera. En dylik analys kan även vara till hjälp i mer generella termer.

Följande rekommendationer bygger på principen att skyddet bör byggas upp av flera lager, att bygga det från ytterkant och inåt och att börja med de komponenter som det är mest troligt blir angripna (de mest skyddsvärda komponenterna) vid en incident. Generellt bör därför först och främst nätverkspunkter med direkt eller indirekt koppling till internet skyddas, vilket lämpligen sker med IDS med nätverksbaserad datainsamling. Därefter bör nyckelfunktioner i det övervakade systemet skyddas. Det kan då handla om till exempel loggservrar och styrenheter. Principen är att först skydda de enheter som har störst förmåga att administrera, styra och kommunicera med andra enheter i

nätverket. Dessa enheter skyddas lämpligtvis med hjälp av ett IDS med värdbaserad datainsamling. Om ytterligare intrångsdetektering behövs är nästa steg att övervaka det interna nätverket, inklusive de processnära delarna. Är det administrativa nätverket (i stort sett) skilt från det processnära nätverket bör ett nätverksbaserat IDS placeras i respektive del, gärna nära de punkter där nätverken är sammankopplade. Måste ett val mellan de två nätverken göras bör det administrativa nätverket skyddas i första hand. Detta bestäms dock av arkitekturen på det aktuella systemet, det vill säga om det administrativa nätverket systemarkitekturmässigt ligger närmare internetkopplingen. Eftersom det ännu inte finns någon större mängd kommersiellt tillgängliga intrångsdetekteringssystem med värdbaserad datainsamlingsfunktion som är processanpassade blir rekommendationen att använda intrångsdetekteringssystem med nätverksbaserad datainsamling i de processnära delarna av det IIS som ska övervakas.

6 Litteraturlista

Abdulhammed, R., Faezipour, M. och Elleithy, K., 2016, Network intrusion dete ction using hardware techniques: A review, *2016 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2016*.

Alajlouni, S., och Rao, V., 2013, Anomaly detection in liquid pipelines using modeling, co-simulation and dynamical estimation, *IFIP International Federation for Information Processing*, **417**; Critical Infrastructure Protection VII, red. Butts, J., Shenoi, S., (Boston: Springer), sid. 111–124.

Bontupalli, V. och Taha, T., 2016, Comprehensive survey on intrusion detection on various hardware and software, *Proceedings of the IEEE National Aerospace Electronics Conference, NAECON* 2016-March, sid. 267–272.

Caselli, M., Zambon, E., Petit, J., och Kargl, F., 2015, Modeling message sequences for intrusion detection in industrial control systems, *IFIP International Federation for Information Processing*, **466**; Critical Infrastructure Protection IX, red. Rice, M., Shenoi, S., (Boston: Springer), sid. 49–71.

Deng, Y., och Shukla, S., 2013, A distributed real-time-event correlation architecture for SCADA security, *IFIP International Federation for Information Processing*, **417**; Critical Infrastructure Protection VII, red. Butts, J., Shenoi, S., (Boston: Springer), sid. 81–93.

Denning, D., 1987, An Intrusion-Detection Model, *IEEE Transactions on Software Engineering* **SE-13**(2), sid. 222–232.

Ganapathy, S., Kulothungan, K., Muthurajkumar, S., Vijayalakshmi, M., Yogesh , P. och Kannan, A., 2013, Intelligent feature selection and classification techniques for intrusion detection in networks: a survey, *EURASIP Journal on Wireless Communications and Networking* **2013**:271.

Hurst, W., Merabti, M., och Fergus, P., 2014, A survey of critical infrastructure security, *IFIP International Federation for Information Processing*, **441**; Critical Infrastructure Protection VIII, red. Butts, J., Shenoi, S., (Boston: Springer), sid. 127–138.

Inayat, Z., Gani, A., Anuar, N., Khan, M. och Anwar, S., 2016, Intrusion respons e systems: Foundations, design, and challenges, *Journal of Network and Computer Applications* **62**, sid. 53–74.

Klump, R., och Kwiatkowski, M., 2010, Distributed IP watchlist generation for intrusion detection in the electrical smart grid, *IFIP International Federation for Information Processing*, **342**; Critical Infrastructure Protection IV, red. Moore, T., Shenoi, S., (Boston: Springer), sid. 113–126.

Liao, H.-J., Lin, C.-H. R., Lin, Y.-C. och Tung, K.-Y., 2013, Intrusion detection system: A comprehensive review, *Journal of Network and Computer Applications* **36**(1), sid. 16–24.

Milenkoski, A., Vieira, M., Kounev, S., Avritzer, A. och Payne, B., 2015, Evaluating computer intrusion detection systems: A survey of common practices, *ACM Computing Surveys* **48**(1).

Mitchell, R. och Chen, I.-R., 2014, A Survey of Intrusion Detection Techniques for Cyber-physical Systems, *ACM Comput. Surv.* **46**(4), sid. 55:1–55:29.

MSB, Myndigheten för samhällsskydd och beredskap, 2014, Vägledning till ökad säkerhet i industriella informations- och styrsystem (MSB718), teknisk rapport, MSB.

MSB, Myndigheten för samhällsskydd och beredskap, 2009, Vägledning till ökad säkerhet i industriella kontrollsystem, teknisk rapport, MSB.

Nai Fovino, I., Masera, M., Guglielmi, M., Carcano, A., och Trombetta, A., 2010, Distributed intrusion detection system for SCADA protocols, *IFIP International Federation for Information Processing*, **342**; Critical Infrastructure Protection IV, red. Moore, T., Shenoi, S., (Boston: Springer), sid. 95–110.

Nazer, G. och Selvakumar, A., 2011, Current intrusion detection techniques in information technology - A detailed analysis, *European Journal of Scientific Research* **65**(4), sid. 611–624.

Oman, P. och Phillips, M., 2008, Intrusion detection and event monitoring in SCADA networks, *IFIP International Federation for Information Processing*, **253**, Critical Infrastructure Protection, red. E. Goetz och S. Shenoi; (Boston:Springer), sid. 161–173.

Peng, Y., Xiang, C., Gao, H., Chen, D., och Ren, W., 2015, Industrial control system fingerprinting and anomaly detection, *IFIP International Federation for Information Processing*, **466**; Critical Infrastructure Protection IX, red. Rice, M., Shenoi, S., (Boston: Springer), sid. 73–85.

Poston, H., 2013, A brief taxonomy of intrusion detection strategies, *National Ae rospace and Electronics Conference, Proceedings of the IEEE*, sid. 255–263.

Reeves, J., Ramaswamy, A., Locasto, M., Bratus, S., och Smith, S., 2011, Lightweight intrusion detection for resource-constrained embedded control systems, *IFIP International Federation for Information Processing*, **367**; Critical Infrastructure Protection V, red. Butts, J., Shenoi, S., (Boston: Springer), sid. 31–46.

Rrushi, J. och Kang, K.-D., 2009, Detecting anomalies in process control networks, *IFIP International Federation for Information Processing*, **311**; Critical Infrastructure Protection III, red. Palmer, C., Shenoi, S., (Boston: Springer), sid. 151–165.

Sen, S., 2015, A Survey of Intrusion Detection Systems Using Evolutionary Co mputation, *Bio-Inspired Computation in Telecommunications*, Yang, X. S., Chien, S. F. & Ting, T. O., red., Elsevier Inc., sid. 73–94.

Sommestad, T., Holm, H., 2016, Test av logganalysverktyget SnIPS, FOI-R--4323--SE.

Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M. och Hahn, A., 2015, Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC) (NIST Special Publication 800-82 (rev. 2)), Technical report, National Institute of Standards and Technology.

Svendsen, N. och Wolthusen, S., 2008, Modeling and detecting anomalies in SCADA systems, *IFIP International Federation for Information Processing*, **290**; Critical Infrastructure Protection II, red. Papa, M., Shenoi, S., (Boston: Springer), sid. 101–113.

Svendsen, N. och Wolthusen, S., 2009, Using physical models for anomaly detection in control systems, *IFIP International Federation for Information Processing*, **311**; Critical Infrastructure Protection III, red. Palmer, C., Shenoi, S., (Boston: Springer), sid. 139–149.

Terminologicentrum, 2017, http://www.tnc.se/termfraga/aktualitet/, läst 2017-03-10

Vasilomanolakis, E., Karuppayah, S., Muhlhauser, M. och Fischer, M., 2015, Taxonomy and survey of collaborative intrusion detection, *ACM Computing Surveys* **47**(4).

Zhu, B. X., 2014, Resilient Control and Intrusion Detection for SCADA Systems, doktorsavhandling, EECS Department, University of California, Berkeley.